HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

DIPLOMARBEIT

Herr

Christopher Petz

Implementierung des Risikomanagementprozesses in der Praxis mit renommierten Methoden aus dem IT-Risikomanagement und der Entscheidungstheorie

Mittweida, 2016

Fakultät Wirtschaftsingenieurwesen

DIPLOMARBEIT

Implementierung des Risikomanagementprozesses in der Praxis mit renommierten Methoden aus dem IT-Risikomanagement und der Entscheidungstheorie

Autor:
Herr

Christopher Petz

Studiengang:
Wirtschaftsingenieurwesen

Seminargruppe:
KW11wIA-F

Erstprüfer:
Prof. Dr. rer. oec. Johannes Stelling

Zweitprüfer:
Prof. Dr. rer. pol., Diplom-Kaufmann Andreas Hollidt

Einreichung:
Mittweida, 29.01.2016

Verteidigung/Bewertung:
Innsbruck, 2016

Faculty Industrial Engineering

DIPLOMATHESIS

Implementation of the Risk Management Process in practice with renowned methods of the IT Risk Management and Decision Theory

author:
Mr.

Christopher Petz

course of studies:
Industrial Engineering

seminar group:
KW11wIA-F

first examiner:
Prof. Dr. rer. oec. Johannes Stelling

second examiner:
Prof. Dr. rer. pol., Diplom-Kaufmann Andreas Hollidt

submission:
Mittweida, 29.01.2016

defence/ evaluation:
Innsbruck, 2016

Bibliografische Beschreibung:

Petz, Christopher:

Implementierung des Risikomanagementprozesses in der Praxis mit renommierten Methoden aus dem IT-Risikomanagement und der Entscheidungstheorie. - 2016. – x, 65, 60, 2 S.

Mittweida, Hochschule Mittweida, (FH), University of Applied Sciences, Fakultät Wirtschaftsingenieurwesen, Diplomarbeit, 2016

Referat:

In dieser Diplomarbeit wird der Risikomanagementprozess im operativen IT-Risikomanagement vorgestellt und mit Instrumenten aus der Praxis empirisch dargestellt. Es wird erarbeitet, ob die Verwendung einer Nutzwertanalyse bzw. Zielprogrammierung zur transparenten Maßnahmenentscheidung im Zuge der Risikosteuerung beitragen kann. Zusätzlich wird geprüft, welcher entscheidungstheoretische Ansatz besser zur Entscheidungsfindung im IT-Risikomanagement geeignet ist.

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BIA	Business Impact Analyse
BSI	Bundesamt für Sicherheit in der Informationssicherheit
EDV	Elektronische Datenverarbeitung
ID	Identifikator
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Informationstechnologie
NWA	Nutzwertanalyse
PDCA	Plan Do Check Act
PoS	Point of Sale
SBK	Schutzbedarfsklasse
SSD	Solid State Disc
SSL	Secure Sockets Layer

1 Einführung

In der modernen Zeit ist vor allem für weltweit agierende Firmen eine gut strukturierte und breit gefächerte IT-Landschaft unabdingbar. Informationstechnologie wird für viele Unternehmenskanäle wie etwa Distributions- und Kommunikationskanäle verwendet und ist inzwischen die Basis vitaler Geschäftsprozesse. Umso größer und schneller wächst die Bedeutsamkeit einer ausfallsicheren und zuverlässigen IT-Infrastruktur. Um den reibungslosen Betrieb sicherstellen zu können, ist es wichtig, Unternehmensrisiken zeitnah zu erfassen, zu bewerten und gegebenenfalls gegenzusteuern, um Schäden zu vermeiden.

„Die unterschiedlichen Erwartungen der Anteilseigner, Belegschaft, Öffentlichkeit, Behörden usw. an die Unternehmen, etwaige Unternehmensrisiken zu bewältigen und über jedes Risiko und die damit einhergehenden Gegenmaßnahmen zur Risikobewältigung zu berichten, erfordern die Etablierung eines gesamtunternehmerischen Risiko- und Chancenmanagements.“[1]

„Die Einführung eines IT-Risikomanagements im Unternehmen ermöglicht es, Bedrohungen frühzeitig zu erkennen, aber auch positive Geschäftsentwicklungen also Chancen aufzudecken.“[2]

[1] (BITKOM, 2006).

[2] Ebd.

1.1 Problemstellung und Motivation aus Sicht eines IT-Sicherheitsverantwortlichen

Die Informationssicherheit gewinnt in modernen Unternehmen zunehmend an Bedeutung und ist ein viel diskutiertes und strittiges Thema. Der stetige und rasche Wandel im Bereich der Informationstechnologie in den letzten Jahren bringt sowohl positive, als auch negative Aspekte im Unternehmensumfeld mit sich. Die fortschreitende Vernetzung von Ressourcen und Endgeräten erleichtert in vieler Hinsicht das tägliche Arbeiten und der Austausch von Daten lässt sich auch ohne fachmännische Kenntnisse einfach gestalten. Doch insbesondere diese Vernetzung von Systemen und der Austausch mit externen Partnern bringt nicht zu unterschätzende Gefahren mit sich. Das Risiko, potenziellen Angreifern und böswilligen Attacken zum Opfer zu fallen, steigt massiv, weshalb auch der Aufwand entsprechende Schutzmaßnahmen und Richtlinien zu definieren, stetig wächst. Im gleichen Zuge steigen die Ansprüche sowohl an IT-Verantwortliche, als auch an die betreuten IT-Systeme selbst. Die Zahl der komplexen Anforderungen, welche von IT-Security-Spezialisten abgesegnet werden müssen, steigt drastisch an und so gilt es als Herausforderung, den Andrang, im Einklang zur Unternehmensstrategie und den IT-Prinzipien, zu bewältigen. Da die Umsetzung IT-relevanter Neuanforderungen oder Systemänderungen in der Regel die Involvierung von IT-Sicherheitsverantwortlichen bedarf, welche auch häufig die finalen Verantwortungen tragen, erfordert es ein Management-Tool, um transparente und nachvollziehbare Entscheidungen an Stakeholder und Kunden kommunizieren zu können. Meist wird die Zustimmung oder Ablehnung eines Antrages zwar schriftlich begründet, jedoch fehlt ein anschauliches Regelwerk, wie es zu dieser Entscheidung kam. Dies ist insbesondere bei nachträglich auftretenden Problemen von äußerster Wichtigkeit, um anschließenden Streitigkeiten vorzubeugen. Vielfach werden risikoreiche Anforderungen durch ihre Dringlichkeit und Nachdruck implementiert oder bestehende Infrastrukturen unzureichend dimensioniert bzw. abgesichert. Das Resultat sind Einsparungen am falschen Ort und implementierte

Lösungen, welche im dauerhaften Betrieb hohe Schäden verursachen können.

1.2 Zielsetzung der Arbeit

In der vorliegenden Arbeit soll die Funktionsweise eines Risikomanagementprozesses näher beleuchtet und mit Hilfe von renommierten Methoden aus der Entscheidungstheorie erweitert werden. Ebenfalls Gegenstand ist dessen Vorgangsweise in der Praxis und die Möglichkeit, Nutzwertanalysen oder Zielprogrammierungen in den Risikomanagementprozess einzubinden. Der Teilprozess der Risikokontrolle wird hier explizit nicht behandelt, da sie Teil des betriebswirtschaftlichen Themengebiets des Risikocontrollings ist. Die Funktionsweisen der Entscheidungsregeln und dessen Vor- und Nachteile sind zudem von besonderem Interesse, um folgenden Forschungsfragen nachzugehen:

Kann die Verwendung einer Nutzwertanalyse oder einer Zielprogrammierung zur transparenteren Risikosteuerung im IT-Risikomanagement beitragen?

Welcher entscheidungstheoretische Ansatz ist im operativen IT-Risikomanagement besser geeignet?

Kern dieser Arbeit ist es gleichermaßen, das Verständnis und die Bedeutsamkeit der Handhabung von IT-Risiken zu vermitteln und die Möglichkeit deren Steuerung um wissenschaftliche Instrumente zu erweitern bzw. transparent zu gestalten.

1.3 Methodisches Vorgehen

Im ersten Teil dieser Arbeit werden die theoretischen Grundlagen nähergebracht, um ein Verständnis der fachspezifischen Begrifflichkeiten aus dem operativen IT-Risikomanagement und der Informationstechnologie aufzubauen. Dabei wird intensiv auf die Notwendigkeiten für das Entstehen eines Risikoszenarios eingegangen, wie etwa das Bestehen einer Schwachstelle und einer Bedrohung. Kapitel 4 ist ganz dem Risikomanagementprozess im operativen Risikomanagementsystem gewidmet, worin die einzelnen Prozessphasen umfangreich analysiert und dargestellt werden. Im Fokus des fünften Kapitels stehen entscheidungstheoretische Ansätze, um aus mehreren Handlungsalternativen auszuwählen. Nach ihrer Eingliederung in die Entscheidungstheorie werden die Verfahren Nutzwertanalyse und Goal-Programming näher beschrieben. Aufbauend auf den Informationen aus dem theoretischen Teil der Arbeit, werden diese Ansätze empirisch und mit Werkzeugen aus der Praxis, am Beispiel dargestellt. Außerdem werden die Nutzwertanalyse und die Zielprogrammierung direkt miteinander verglichen. Abschließend werden die Ergebnisse der Arbeit dargelegt, die Forschungsfragen beantwortet und vom Autor kritisch betrachtet.

2 Fundamentale Definitionen und Abgrenzungen

Im folgenden Kapitel werden bereits publizierte Definitionen und Abgrenzungen aus dem Risikomanagement und der Informationstechnologie verständlich erläutert und zusätzlich mit eigenen Definitionen und Abgrenzungen erweitert. Durch diese Herangehensweise soll die Komplexität reduziert werden, da viele Begrifflichkeiten nicht klar umrissen bzw. konkretisiert sind und recht unterschiedlich interpretiert werden können.

2.1 Erläuterung des Risikomanagements und Risikobegriffs

Der Begriff Risikomanagement stammt ursprünglich aus der Finanzwelt und fand mit zunehmender Bedeutsamkeit der EDV auch Einzug in die Unternehmens- und Informationstechnologie. In der Regel wird das Risikomanagement in zwei Arten gegliedert: Enterprise Risk Management (ERM) oder in ein traditionelles Risikomanagement. Das Enterprise Risk Management beschäftigt sich mit einem globalen, ganzheitlichen Ansatz zur Steuerung von Risiken und Chancen, wohingegen sich das traditionelle Risikomanagement lediglich mit einzelnen Sub-Bereichen (Geschäftsbereiche, Unternehmensstrukturen etc.) befasst wie z.B. das in dieser Arbeit behandelte IT-Risikomanagement.

Ziele des IT-Risikomanagements können wie folgt in allgemeiner Weise nach Seibold beschrieben und definiert werden:[3]

- Mitarbeiter für Risiken sensibilisieren.
- Eine Risikokultur bilden.
- Transparenz der Risikosituation herstellen.

[3] (Seibold, 2006).

- Risiken auf ein akzeptables Maß reduzieren bei gleichzeitig möglichst geringer Beschneidung der Chancen.

Für den Begriff „Risiko“ lassen sich hingegen viele unterschiedliche Definitionen finden, so beschreibt Duden das Risiko als einen negativen Ausgang bei einer Unternehmung, mit dem Nachteile, Verlust oder Schäden verbunden sind.[4] „Unter Risiko versteht man auch die nach Häufigkeit (Eintrittserwartung) und Auswirkung eingeschätzte, konkrete Bedrohung eines Systems bzw. einer Organisation.“[5]

Abbildung 1: Risikofunktion[6]

Beim IT-Risikomanagement wird die Risikofunktion in der Regel durch einen Erwartungswert dargestellt.

Hierbei wird das Risiko als numerischer Wert durch die Multiplikation zweier Faktoren beschrieben, was den Vorteil einer leichteren Vergleichbarkeit mehrerer, unterschiedlicher Risiken bietet:

„**Risikoerwartungswert = Eintrittswahrscheinlichkeit * Auswirkung**“[7]

Die Simplizität dieser Formel birgt jedoch auch eine erhebliche Gefahr mit sich, da seltene Ereignisse mit besonders großer Auswirkung bzw. Schadenswert, nur ein mittleres, wenn nicht sogar ein geringes Risiko ergeben würde.[8] „Dies

[4] Vgl. (Duden, 2015).

[5] (Vorest AG, 2014).

[6] Ebd.

[7] (Schröder).

[8] Vgl. (Krausz, 2005).

führt zu einer Unterschätzung der tatsächlichen Situation, wobei die Frage des Zeitpunktes, also wann der Schaden genau eintreten wird, vollständig vernachlässigt wird und in menschlicher Denkweise oft die Tatsache einer Wahrscheinlichkeit von z.B.: 10^{-16} dazu verleitet, zu glauben der Schaden würde erst nach 10^{-16} Zeiteinheiten eintreten."[9]

2.2 Einführung in die IT Prinzipien

„Im Informationssicherheitsmanagement geht man grundsätzlich vom modernen Risikobegriff [zweidimensionale Sichtweise -> stets präsente Bedrohung wirkt auf eine gegenwärtige Schwachstelle im System] aus und erweitert diesen auf die Sphären **Vertraulichkeit**, **Verfügbarkeit** und **Integrität**."[10] Da bei global tätigen Unternehmen die Einhaltung länderspezifischer Gesetzgebungen (vor allem in Punkto Datenschutzrichtlinien) unerlässlich ist, können diese drei Dimensionen zusätzlich mit der, der **Rechtskonformität** ausgedehnt werden. Diese Sphären werden in der Regel im IT-Umfeld als IT-Prinzipien oder IT-Grundsätze bezeichnet. Diese Arbeit beschränkt sich jedoch auf die klassischen Drei.

Unter dem Begriff **Vertraulichkeit** wird im IT-Komplex der Schutz von Daten gegenüber Unbefugten verstanden. Dies bedeutet, dass z.B. lediglich der Sender und der Empfänger Zugriff auf bestimmte Datenpakete haben, was etwa durch den Einsatz einer geeigneten Verschlüsselung erreicht werden kann. Der Terminus „Vertrauen" wird jedoch nicht nur im Zusammenhang „Datenschutz vor Unbekannten" verwendet, sondern findet vor allem auch bei der Berechtigungsvergabe und Zugriffsverwaltung innerhalb eines Unternehmens häufig Gebrauch. „Die Vertraulichkeit ist also ein Maß dafür, inwieweit gewährleistet wird, dass eine vertrauliche Information nur denjenigen Personen zugänglich gemacht wird, für die sie vorgesehen ist."[11]

---

[9] Ebd.

[10] Ebd.

[11] (Schmidt, 2006).

Die **Verfügbarkeit** ist eine wirtschaftliche Komponente, welche sich gleichermaßen auf Systeme und deren Funktionalität, sowie auf Daten oder Informationen bezieht.[12] Der Bewertungsmaßstab dieses IT-Prinzips wird überwiegend aus IT-Architektur-Richtlinien und aus IT-Security-Richtlinien abgeleitet, wobei organisatorische Regelung zur Betreuung der Anwendungen, welche auf den betroffenen Systemen laufen, zusätzlich mitberücksichtigt werden müssen.[13] Da bei einem Ausfall essentieller Systeme ein hoher wirtschaftlicher Schaden entstehen kann, sind Datenverarbeitungssysteme und Kommunikationswege in der Regel redundant ausgeführt[14]; man spricht von einer Hochverfügbarkeit. Ein Beispiel für in der Regel redundant ausgelegte Systeme wäre die Exchange-Infrastruktur eines Unternehmens, da bei einem Ausfall dieser, einer der wichtigsten Kommunikationskanäle nicht zur Verfügung stehen würde.

Ein weiteres, wichtiges Prinzip der IT-Security wird **Integrität** genannt. Bei vollkommener Integrität einer Nachricht kann davon ausgegangen werden, dass der Nachrichteninhalt auf der Sende- und Empfangsseite vollkommen identisch ist, also der Nachrichteninhalt bei der Übertragung unverändert geblieben ist.[15] Die Integrität beschreibt also einen Wert, in welchem Maße, bestimmte Informationen ihren ursprünglichen Zustand behalten. Da jegliche Abweichung vom Ausgangswert hohe Risiken mit sich bringt, werden stetig neue Techniken und Methoden zur Sicherstellung des Ausgangswertes entwickelt.

[12] Vgl. (ITWissen, 2014).

[13] Vgl. (Seibold, 2006).

[14] Vgl. (ITWissen, 2014).

[15] Vgl. Ebd.

2.3 Abgrenzung des Risikos von der Chance

Zunächst scheinen die Begriffe „Risiko“ und „Chance“ im Volksmund recht unterschiedlich, jedoch sind sie sich grundlegend sehr ähnlich. Eine klare Definition des Chancenbegriffs ist schwer festzulegen, da in der Literatur verschiedenste Interpretationen und Explikationen zu finden sind. „Risiko“ wird in unserer Gesellschaft sehr oft mit etwas Negativen in Verbindung gebracht, wohingegen die Chance als sehr positiv erachtet wird. Es gibt jedoch durchaus Menschen, welche das Gefühl beim Akzeptieren eines Risikos, gegensätzlich zur Allgemeinheit, als erfreulich schildern würden. Als Beispiel sei hier der Sprung mit Fallschirm aus dem Flugzeug zu nennen. Das Risiko, dass der Fallschirm nicht aufgehen könnte und der damit verbundene Nervenkitzel schütten Unmengen an Adrenalin in uns aus, welches wir als Glücksgefühle wahrnehmen. Keiner würde hier das Nicht-Öffnen des Fallschirms als Chance bezeichnen. Grundlegend jedoch beschreiben beide Bezeichnungen eine Zustandsentwicklung, welche sowohl ein negatives als auch ein positives Resultat liefern kann. Risiko und Chance sind zweifellos eng miteinander verbunden. Im Unternehmensumfeld sind fast immer Risiken zu akzeptieren bzw. zu minimieren, bevor Chancen genutzt werden können. So ist etwa für das Verlegen des eigenen Rechenzentrums in die Cloud (hier als Chance um z.B.: den administrativen Aufwand zu reduzieren), das Risiko hinsichtlich Datenschutz vorab abzuwägen und notfalls zu tolerieren.

2.4 Entstehung und Auswirkungen von Risiken

Im folgenden Abschnitt soll das Entstehen von Risiken und deren Auswirkungen auf die Umwelt näher erläutert werden. Dies ist essentiell, um Gefahren qualitativ zu bewerten und ihre Relevanz im operativen Risikomanagement einordnen zu können.

2.4.1 Präzisieren von Schwachstellen im IT-Risikomanagement

Die Voraussetzung für das Entstehen eines Sicherheitsrisikos ist das Bestehen einer Schwachstelle. Ist keine Schwachstelle vorhanden, so kann auch kein Risiko generiert werden. (Es existiert eine interdependente Beziehung) „Der Begriff Vulnerability, zu Deutsch Schwachstelle, wird in der Informationssicherheit [leider zu häufig] in dem Sinne benutzt, als dass es sich um einen Fehler der Software handelt, der von Hackern genutzt werden kann und ihnen den Zugriff auf Systeme oder Netzwerke ermöglicht.“[16] Diese Erläuterung einer Schwachstelle beschreibt jedoch lediglich einen Schwachstellentyp und sollte nicht als allgemeingültige Definition verstanden werden. Vulnerabilities können besser als Eigenschaften von Objekten innerhalb der IT beschrieben werden und können sowohl technischer, organisatorischer, als auch personeller Natur sein.[17] Das Identifizieren der Schwachstellen – unabhängig ihres Typus- nimmt in der Realität sehr viel Zeit in Anspruch, da in Wirklichkeit nicht nur eine Vielzahl an Schwachstellen in einem Unternehmen bzw. IT-Service existieren, sondern auch stetig (fast täglich) Neue hinzukommen und Bestehende sich verändern. „Es ist in der Praxis fast unmöglich, auf jeden Fall aber wirtschaftlich nicht vertretbar, alle Schwachstellen zu kennen bzw. ermitteln zu wollen.“[18]

Mit Hilfe einer Schwachstellenanalyse lässt sich erkennen, dass sowohl generisch anwendbare, als auch umwelt- bzw. systemspezifische Schwachstellen existieren. Außerdem werden die Schwachstellen ökonomisch priorisiert und ihrer Bedrohung zugeordnet.

---

[16] (ITWissen, 2015).

[17] Vgl. (Schmidt, 2006).

[18] (Schmidt, 2006).

a) *Technische Schwachstellen:*

Das Bestehen technischer Schwachstellen ist in der Regel am einfachsten nachzuvollziehen und vor allem für den Systemadministrator jener Typ, welcher ihm als erster in den Sinn kommt, da auf größere, technische Vulnerabilities auch in den Medien hingewiesen wird. Ein prominentes Beispiel hierfür wäre der viel diskutierte Heartbleed Bug, welcher ein schwerwiegender Programmfehler in älteren Open-SSL Versionen ist. Weitere technische Schwachstellen sind defekte Datenträger, Softwarefehler oder auch der Ausfall von Systemkomponenten.

b) *Organisatorische Schwachstellen:*

„Organisatorische Schwachstellen ergeben sich aus aufbau- oder ablauforganisatorischen Festlegungen oder deren Fehlen, z.B. das Fehlen einer klaren Vertretungsregelung im Urlaubs- bzw. Krankheitsfall.“[19] Fehler in der Zutrittskontrolle oder gefährliche Arbeitsbedingungen gehören ebenfalls zu den organisatorischen Schwachstellen.

c) *Personelle Schwachstellen:*

Personelle Schwachstellen sind überwiegend auf menschliches Versagen bzw. menschliches Fehlverhalten zurückzuführen. Wird etwa der Zugang zum Datenzentrum eines Unternehmens vom zuständigen Mitarbeiter nicht ordnungsgemäß beim Verlassen des Raumes verriegelt, so Besteht die Möglichkeit des Missbrauchs für Dritte. Bedienungsfehler und Fahrlässigkeit zählen ebenso zu den personellen Schwachstellen.

[19] (Krallmann, et al., 2002).

2.4.2 Die Schwachstelle und der Angriffspfad als eine Einheit

„Grundsätzlich gilt, dass ein System nur dann einer Bedrohung ausgesetzt ist, wenn es eine Schwachstelle hat und eine Möglichkeit existiert, diese auszunutzen.“[20] Um diese Schwachstelle ausnutzen zu können, muss jedoch in jedem Falle ein ununterbrochener bzw. vollständiger Angriffspfad bestehen. Dies kann in der Praxis wie folgt an einem Beispiel veranschaulicht werden:

Angenommen ein Client mit Betriebssystem XY wurde nicht mit den letzten, monatlichen Security-Patches versorgt. Einer dieser Patches hätte eine kritische Sicherheitslücke im Betriebssystem geschlossen, mit Hilfe derer sich ein Angreifer durch Ausführen eines Schadcodes Administratorenberechtigungen erschließen könnte. Um diesen Schadcode auszuführen, wird Zugriff über das Netzwerk auf den Client benötigt, welcher hier den Angriffspfad darstellt. Angenommen dieser Client würde nun über keinerlei Netzwerkanbindung verfügen, so würde der Angriffspfad unterbrochen bzw. nicht existieren und die kritische Sicherheitslücke / Schwachstelle kann nicht ausgenutzt werden. Die Schwachstelle und der Angriffspfad bilden somit eine Einheit und bei Nichtbestehen eines Angriffspfades sind jene Schwachstellen zu vernachlässigen (siehe *Abschnitt 4.2*).

2.4.3 Die Entstehung einer Bedrohung

Auch wenn eine Schwachstelle in Kombination mit einem dezidierten Angriffspfad vorliegt, so braucht es ein weiteres Glied, um ein Risikoszenario zu bilden und zwar eine aktive bzw. akute, reale Bedrohung. „Es kann sich dabei um ein Ereignis handeln, das Schaden verursacht, um einen Angriff auf ein System, eine Übertragungsstrecke oder auf den Informationsinhalt einer Nachricht, um Spionage oder Sabotage oder auch um Gefahren, die unbeabsichtigt oder durch natürliche Ereignisse wie Stromausfall, absichtlich

[20] (Harich, 2015).

oder vorsätzlich von Mitarbeitern ausgehen."[21] In jedem Falle muss die Bedrohung aktuell sein und zum Zeitpunkt des Erfassens bestehen d.h. für das Beispiel aus 3.4.2 gilt folgendes:

Besteht die Sicherheitslücke und der Client ist mit dem Internet verbunden, so existiert erst eine Bedrohung, wenn ein potenzieller Angreifer vorliegt und dieser das Interesse hat, die Sicherheitslücke zu verwenden, um Schadcode auszuführen (Diebstahl von Kreditkartendaten). Eine Bedrohung kann dabei mehrere, unterschiedliche Schwachstellen aufweisen.

2.4.4 Die Bildung eines Risikoszenarios und seine Auswirkung

Wie bereits erwähnt, bedarf es drei Voraussetzungen zur Entstehung eines Risikoszenarios:

- Mind. eine Schwachstelle.
- Die Möglichkeit diese Schwachstelle auszunutzen (Angriffspfad).
- Eine aktive, reale Bedrohung.

Unter dem Begriff Risikoszenario wird das ganzheitliche Aufzeigen von möglichen Schadensabläufen anhand von generischen Beispielen verstanden, um deren Auswirkung bzw. das Schadensausmaß besser abwägen zu können.[22] Jegliche Veränderung der drei Komponenten (Schwachstelle, Angriffspfad, Bedrohung) oder eine Modifikation der Systemlandschaft führt zur Abwandlung des Risikoszenarios wie z.B.: *„Die Einführung einer weiteren Sicherheitskomponente in die Systemlandschaft erhöht deren Komplexität und wirkt sich risikoerhöhend auf alle Risikoszenarien […] aus."*[23]

Dies ist bei der späteren Behandlung von Risiken zu beachten.

---

[21] (ITWissen, 2015).

[22] Vgl. (Seibold, 2006).

[23] Ebd.

3 Der Risikomanagementprozess im operativen Risikomanagementsystem

Nachstehend wird der Risikomanagementprozess als Kernkomponente eines jeden Risikomanagementsystems verdeutlicht. „Der Risikomanagementprozess wird in zwei wesentliche Bestandteile untergliedert: das strategische Risikomanagement und das operative Risikomanagement.“[24] „Strategisch“ bedeutet das weitsichtige Handeln aufgrund gesammelter Informationen (in der Praxis häufig „Weak Signals“ genannt) und der Beurteilung wirtschaftlicher Trends. Das operative Risikomanagement befasst sich hingegen mit spezifischen Kennzahlen und beinhaltet im Wesentlichen die Identifikation, Bewertung, Steuerung und Kontrolle von Risiken. So können Bedrohungen effektiv begrenzt, vermindert und bestenfalls vermieden werden. Die strategische und operative Komponente bilden schließlich gemeinsam ein in sich geschlossenes System, was die Vorteile einer besseren Fundierung von unternehmerischen Entscheidungen und einer langfristigen Sicherung durch Ausbalancieren der Chancen und Risiken bietet. Diese strategische Komponente macht jedoch nur beim Betreiben des anfangs erwähnten „Enterprise Risk Managements“ Sinn, da hier nicht nur das IT-Risikomanagement behandelt wird, sondern die Gesamtheit aller unternehmerischen, relevanten Faktoren miteinbezogen werden. -> somit wird hier lediglich der operative Part des Risikomanagementprozesses beleuchtet.

3.1 Darstellung des Risikomanagementprozesses

Wie bereits eingehend erwähnt, ist der Risikomanagementprozess ein wichtiges Bauteil im Risikomanagementsystem.

[24] (Balduin, et al.).

„Ein Risikomanagementsystem hat sicherzustellen, dass Risiken, die den unternehmerischen Erfolg und insbesondere den Fortbestand der Unternehmung gefährden, frühzeitig erkannt und gesteuert werden.“[25]

Exakt diese Intention des Systems spiegelt sich im Risikomanagementprozess wider. Dieser Prozess besteht aus vier Phasen, welche zyklisch miteinander verbunden sind und so schlussendlich einen Kreislauf ähnlich dem PDCA-Zyklus nach Deming bilden: Risikoidentifikation, Risikobewertung, Risikosteuerung und Risikokontrolle.

Abbildung 2: Risikomanagementprozess; [eigene Darstellung]

Das Prozessziel ist das Senken bzw. (falls möglich) das Vermeiden von Risiken mit dem Einsatz individuell gestalteter Maßnahmen. „Prozessbegleitend ist eine Risikokommunikation im Unternehmen erforderlich, die eine rechtzeitige Weiterleitung der relevanten Informationen an die jeweils Verantwortlichen sicherstellt und das Risikobewusstsein in der Unternehmung stärken soll.“[26] Die

[25] (Reichling, et al.).

[26] (Gabler, 2015).

Prozessphasen, ausgenommen der Risikokontrolle, werden nun anschließend genauer erörtert.

3.2 Die Identifikation von Risiken im Risikomanagementprozess

„Die Prozessphase der Risikoidentifikation umfasst eine möglichst vollständige und kontinuierliche Erfassung aller Gefahrenquellen, Störpotenziale und Schadensursachen eines Unternehmens, die sich negativ auf das Erreichen der Unternehmensziele (etwa die Steigerung des Unternehmenswertes) auswirken können."[27]

Dabei ist zu beachten, dass Bedrohungen immer entsprechend vorhandene Schwachstellen und Angriffspfade benötigen, um ungewollte Situationen zu ermöglichen. Daraus folgt, dass zu einer ausführlichen Risikoidentifikation auch eine Analyse der prozessinternen Schwachstellen (Schwachstellenanalyse) vonnöten ist.

Im Zuge einer Schwachstellenanalyse werden Schwachstellen und Angriffspfade strukturiert gegliedert, beschrieben und anschließend den Bedrohungen zugeordnet:

Bedrohung	Schwachstelle	Angriffspfad
Diebstahl von Kreditkartendaten	ungepatchte Java-Sicherheitslücke	Applikation tauscht Daten über das Internet aus
	veraltete SSL-Verschlüsselung	Dateneingabe über unsichere Verbindung

Tabelle 1: Beispiel einer einfachen Schwachstellenanalyse

[27] (Romeike, et al.).

Eine Bedrohung kann dabei auch mehrere Schwachstellen mit unterschiedlichen oder gleichen Angriffspfaden besitzen. Da alle erforderlichen Parameter vorliegen, kann ein Risiko deklariert werden z.B.: die unwillkürliche Behebung von Geld durch Dritte. Dieses Risiko wirkt sich folglich auf das IT-Prinzip der Vertraulichkeit aus. Sind alle Risiken identifiziert, werden sie anhand eines Risikoprotokolls mit all ihren Parametern dokumentiert und erhalten eine Kennung. Die Risiko ID sollte dabei immer anhand einer unternehmensweit gültigen Namenskonvention aufgebaut sein.

Risiko ID	XXX-XXX-XXX-X.X (Namenskonvention)
Risikoszenario	
Risikoauswirkung auf	*Vertraulichkeit* ☐ *Integrität* ☐ *Verfügbarkeit* ☐
Risikoträger	
Beischreibung des Risikoszenarios	*Schwachstelle :* *Bedrohung:* *Auswirkung:*

Tabelle 2: Einfaches Risikoprotokoll

Außerdem ist es wichtig bei der Risikoidentifikation einen Risikoträger zu ermitteln. Er ist verantwortlich für Schäden, welche beim Eintritt des Risikoszenarios entstehen können. Nach jeder Phase des Risikomanagementprozesses wird das Risikoprotokoll mit den Ergebnissen aus dem jeweiligen Abschnitt erweitert, um eine vollständige Dokumentation der Risikoanalyse zu erhalten.

Wahrscheinlichkeit	*Sehr Hoch* ☐ Erwartetes Auftreten des Risikos innerhalb der nächsten drei Monate sehr wahrscheinlich. Hohe Anzahl an Störungen erwartet. *Hoch* ☐ Erwartetes Auftreten des Risikos innerhalb von sechs Monaten. Mittelmäßige Anzahl an Störungen erwartet. *Mittel* ☐ Erwartetes Auftreten des Risikos innerhalb der nächsten zwölf Monate. Geringe Anzahl an Störungen erwartet. *Niedrig* ☐ Erwartetes Auftreten des Risikos innerhalb von 24 Monaten sehr unwahrscheinlich. Es werden keine Störungen erwartet.
Gegenmaßnahme(n) (gewählte Risikostrategie)	*Risikostrategie und gewählte Maßnahme(n):* *Kosten:* *Start der Umsetzung (falls zutreffend):* *Geplantes Ende der Umsetzung (falls zutreffend):* *Verbleibendes Restrisiko:* Ja ☐ *[Beschreibung des Restrisikos]* Nein ☐

Tabelle 3: Erweitertes Risikoprotokoll

Die umfangreiche Deklaration eines Einzelrisikos ist erforderlich, um alle involvierten Personen auf denselben Wissensstand zu bringen und um Missverständnisse zu vermeiden.

3.3 Die Risikobewertung im Detail

Das Charakterisieren von Risiken ist essentiell für den Risikomanagementprozess, weshalb eine gründliche Vorgehens- und Arbeitsweise maßgeblich für den gesamten Prozess ist.

„Die Prozessphase der Risikobewertung basiert auf den Ergebnissen der Risikoidentifikation und umfasst eine möglichst vollständige und kontinuierliche qualitative Beurteilung und quantitative Bewertung aller identifizierten Risiken.“[28]

Ein Risiko qualitativ zu beurteilen bedeutet, es mit Hilfe von ordinalen Kennzahlen wie z.B.: selten, häufig, stark, mittel, katastrophal etc. zu beschreiben, wohingegen bei einer quantitativen Bewertung mit eindeutig definierten Größen wie z.B.: Schadenshöhe in Euro, Eintrittswahrscheinlichkeit (Anzahl pro Zeiteinheit) etc. gearbeitet wird.[29] Die Basis zur Berechnung mit Hilfe des Risikoerwartungswertes wurde bereits im *Abschnitt 3.1* behandelt, weshalb nun das Veranschaulichen mittels einer Risikomatrix geschildert wird.

Hierbei werden Bedrohungen einzeln nach ihrer Auswirkung bzw. Schadenshöhe und ihrer Eintrittswahrscheinlichkeit in einem kartesischen Koordinatensystem eingetragen. Dies soll als Hilfsmittel zur besseren Kategorisierung der Risiken und zur Beibehaltung des Überblicks dienen. Dabei wird entlang der Abszissenachse die Eintrittswahrscheinlichkeit in Prozent und auf der Ordinatenachse die Auswirkung bzw. die Schadenshöhe eingetragen. Der Schnittpunkt beider Größen, ergibt die Lage des behandelten Risikos. Risiken, welche ein sehr hohes Schadenspotenzial besitzen, sollen ebenso vermieden werden, wie etwa jene, mit einer hohen Eintrittswahrscheinlichkeit. Daraus folgt, dass Risiken mit geringen Faktorwerten (**R=L*I**)[30] eher zu akzeptieren

---

[28] (Romeike, et al.).

[29] Vgl. (Preiss).

[30] Risk = Likelihood * Impact (z.Dt.: Risiko= Eintrittswahrscheinlichkeit * Auswirkung).

sind. In der Praxis lassen sich nicht alle Risiken komplett vermeiden, sondern es kann lediglich eine Risikostrategie verfolgt werden.

3.4 Die Steuerung von Risiken und ihre strategischen Aspekte

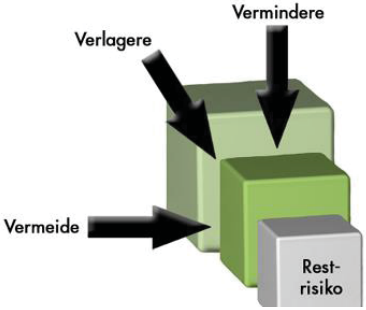

Abbildung 3: Risikostrategien [Vorest AG]

Wie bereits im vorherigen Abschnitt erläutert, ist es erforderlich, ökonomische und strategische Handlungsalternativen für den Umgang mit Risiken aufzuweisen.

Die Relevanz einer geeigneten Entscheidung aus diesen Alternativen bzw. auch Risikostrategien genannt, kann an einem Beispiels aus der Kosteneffizienz von Ortwin Renn sehr gut dargestellt werden:

„Würde es sich lohnen, nicht belasteten Fisch so zu subventionieren, dass die dafür anfallenden Kosten geringer sind als die Kosten, die aufgrund des Verzehrs belasteter Fische auftreten würden?“[31]

Daraus lassen sich in der Praxis vier Risikostrategien ableiten:

- *Risikoakzeptanz*
- *Risikoreduktion*
- *Risikotransfer*
- *Risikovermeidung*

Um zwischen den unterschiedlichen Strategien, vor allem zwischen Risikoakzeptanz und Risikoreduktion, wählen zu können, bedarf es einer Richtlinie, welche Risiken eingegangen werden. Dieses Maß wird Risikobereitschaft genannt.

[31] (Renn, 2005).

3.4.1 Die Risikobereitschaft

In welcher Art und Weise bzw. ob Risiken überhaupt behandelt werden, wird über die Risikobereitschaft geregelt, welche je nach Unternehmung oder persönlicher Interessen variieren kann. Diese Risikobereitschaft muss vorab vom Risikoträger definiert und kommuniziert werden. Sie wird anschließend in einem Risikodiagramm eingetragen, wodurch es in zwei Hälften getrennt wird. In der Regel verläuft diese Trennlinie (hier in rot) von links nach rechts fallend:

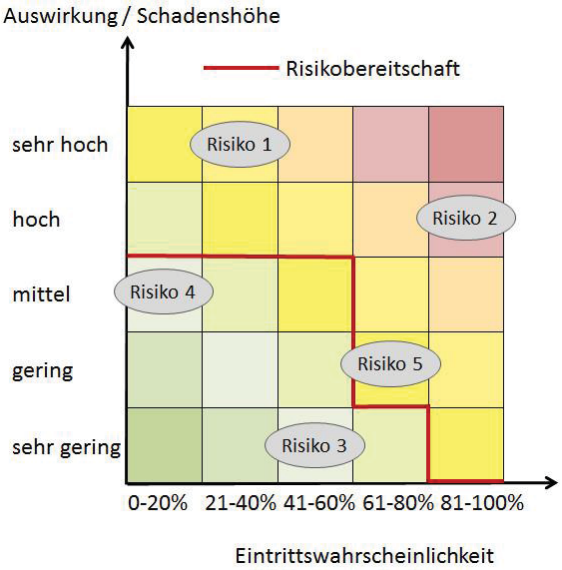

Abbildung 4: Risikobereitschaft[32]

Der untere Teilbereich spiegelt nun die Risikoakzeptanz wider und innerhalb des oberen Abschnitts befinden sich alle zu behandelnden Risiken, da ihr aktueller Wert den Grenz- bzw. Toleranzbereich überschreitet.

[32] (Angermeier, 2014).

Es kann jedoch durchaus vorkommen, dass sich Risiken nicht unter den zuvor definierten Grenzbereich verschieben lassen. Zwei Gründe hierfür könnten zum Beispiel folgende sein:

- *Eine schlechte Rentabilität aus Investment und Resultat*
- *Risiken lassen sich schlichtweg weder vermeiden, noch reduzieren*

Ein besonderes Augenmerk sollte in jedem Falle auf das Verhältnis vom eingesetzten Aufwand zum größtmöglich eintretenden Schaden gelegt werden. Aufwand ist in der Praxis nicht selten mit Arbeit oder Investitionen in Form von Gütern oder Geldmitteln gleichzusetzen. In der Regel spricht man dann vom Risiko-Nutzen-Vergleich, welcher gewöhnlich durch Erfahrungswerte geschätzt wird. Die eingesetzten Mittel sollten nie das denkbar höchste Schadensausmaß überschreiten. Ausgenommen sind hier einige wenige Ausnahmen, wenn etwa Menschenleben gefährdet sind.

3.4.2 Das Akzeptieren von Risiken

Risiken können, sofern deren Auswirkung die IT-Grundsätze nicht in hohem Maße beeinträchtigen bzw. deren Schutzbedarfsklasse (siehe Abschnitt 6.1.4) nicht größer gleich „Hoch“ beurteilt wurden, vom Risikoverantwortlichen akzeptiert werden. – Es werden keine weiteren Schutzmaßnahmen erarbeitet – Dies kann etwa nach Renn’s Exempel gelten oder wenn die Auswirkungen der ausgehenden Bedrohung zu gering sind.

3.4.3 Die Reduktion von Risiken auf ein bestimmtes Maß

Die Verringerung von Risiken wird durch das Design und die Umsetzung technischer oder organisatorischer Gegenmaßnahmen erreicht. Diese Gegenmaßnahmen reduzieren in der Regel die Eintrittswahrscheinlichkeit oder die möglichen Auswirkungen. Zur Risikoreduktion werden bestimmte Rahmenparameter festgelegt (ähnlich der Risikobewertung), um wiederum ein

effizientes Risikomanagement betreiben zu können. Zur transparenten Nachvollziehbarkeit können renommierte Methoden aus der Entscheidungstheorie (Nutzwertanalyse, Goal-Programming) verwendet werden.

3.4.4 Der Transfer von Risiken

Eine weitere Option der Risikostrategie ist das Übertragen von Risiken auf andere interne oder betriebsexterne Rechtspersonen bzw. Institute. Dies wäre möglich, wenn die Reduktion des identifizierten Risikos auf ein akzeptables Level nicht erreichbar bzw. auf einer operationalen und finanziellen Basis nicht rentabel ist. Eine übliche Methode für einen solchen (finanziellen) Transfer wäre die Risikoübertragung auf Versicherungsgesellschaften.

3.4.5 Das Vermeiden von Risiken

Manchmal lassen sich Risiken schlichtweg weder akzeptieren oder reduzieren, noch transferieren. In diesem Fall kann es durchaus Sinn machen, die risikobehaftete Unternehmung zu unterlassen. Als Beispiel wäre hier ein Verbot des Datenaustausches außerhalb des Firmennetzwerkes zu nennen.

4 Die Entscheidungstheorie als Instrument im IT-Risikomanagement

Die Entscheidungstheorie kann als Werkzeug zur Evaluation von Entscheidungen verstanden werden und lässt sich, je nach dem im Vordergrund stehenden Forschungsziel, zwischen deskriptiver, präskriptiver und normativer Entscheidungstheorie unterscheiden.[33] Stammend aus der Betriebswirtschaft, hat sie auch in vielen Teilbereichen, wie etwa des Risikomanagements, Einzug genommen und sich etabliert. Weitere Anwendungsgebiete der Entscheidungstheorie sind: Auswahl der Rechtsform, Investitionsplanung, Standortwahl und die Rohstoffexploration.[34] Im folgenden Kapitel sollen die fundamentalen Gedanken, das Leitmotiv und ein Teil der Entscheidungstheorie, verständlich dargelegt werden. Insbesondere werden Entscheidungen unter Sicherheit und mehrdimensionale Entscheidungsprobleme beleuchtet, da diese nachfolgend und an einem Beispiel zur Maßnahmenentscheidung, herangezogen werden. Schließlich soll der Zusammenhang zwischen ausgewählten Entscheidungsregeln, der Unternehmensstrategie und deren Relevanz verdeutlicht werden.

4.1 Die Basis der normativen Entscheidungstheorie

Ziel der normativen Entscheidungstheorie ist die Auswahl einer von mehreren Alternativen, durch klar definierte Regeln, bei gegebenen Umweltzuständen und Eintrittswahrscheinlichkeiten.[35] Basis der Entscheidungstheorie bilden vorhandene Entscheidungsprobleme, welche im Allgemeinen durch eine sogenannte Ergebnismatrix und spezifische Entscheidungsregeln dargestellt

[33] Vgl. (Gabler, 2015).

[34] Vgl. (Stelling, 2009).

[35] Vgl. (Fleßa, 2015).

werden können. „Die Zeilen der Tabelle repräsentieren die Handlungsalternativen, die Spalten die Umweltzustände, und in den einzelnen Zellen werden die Ergebnisse abgetragen.“[36]

	S1	**S2**	**S3**
A1	80	180	40
A2	40	20	40

Tabelle 4: Ergebnismatrix der Entscheidungstheorie [eigene Darstellung]

Durch den Einsatz der gewünschten Entscheidungsregel, lässt sich nun aus den Umweltzuständen S1, S2 & S3 die geeignetste Alternative A1 oder A2 wählen.

4.2 Entscheidungen unter Sicherheit treffen

Entscheidungen können unter verschiedenen Umweltsituationen / Fallausprägungen getroffen werden, wie etwa „unter Sicherheit“, „unter Ungewissheit“, „unter Risiko“ oder „in einer Spielsituation“.[37] „Entscheidungen „unter Sicherheit“ werden dann getroffen, wenn der in der Zukunft eintretende Umweltzustand bekannt ist oder vom Eintreten einer bestimmten Prognose ausgegangen wird.“[38] „Sicherheit lässt sich […] als der Fall beschreiben, indem nur ein relevanter Umweltzustand vorliegt.“[39]

[36] (Gabler, 2015).

[37] Vgl. (Stelling, 2009).

[38] (Fink, et al., 2011).

[39] (Obermaier, et al., 2013).

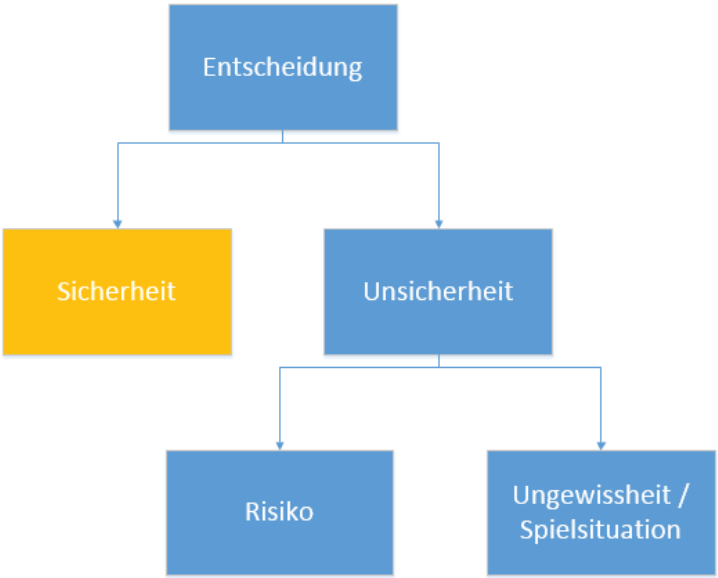

Abbildung 5: Umweltsituationen einer Entscheidung [eigene Darstellung]

„Man wird in den wenigsten Fällen alles wissen, was man wissen müsste, um eine Entscheidung unter „Sicherheit" treffen zu können (die Annahme vollkommener Information ist für viele Entscheidungssituationen nur theoretischer Natur)."[40] Die in dieser Arbeit behandelten Entscheidungsregeln sind den Entscheidungen unter Sicherheit zuzuordnen, weshalb Entscheidungsprobleme unter Unsicherheit nicht näher betrachtet werden.

[40] (Meixner, et al., 2010).

4.2.1 Eindimensionale Entscheidungsprobleme

Eindimensionale Entscheidungsprobleme liegen dann vor, wenn nur ein Ziel verfolgt wird. Dieses Ziel kann entweder fixiert (begrenzte Zielsetzung) oder nicht fixiert (unbegrenzte Zielsetzung) werden. Eine unbegrenzte Zielsetzung strebt entweder eine Maximierung oder eine Minimierung der Zielausprägung an, wohingegen bei einer begrenzten Zielsetzung ein fixierter Wert bzw. ein fester Wertebereich erwartet wird und jene Alternative gewählt wird, deren Zielausprägung den festen Werten am ehesten entspricht.[41]

4.2.2 Mehrdimensionale Entscheidungsprobleme unter Sicherheit

„Bei mehrdimensionalen Entscheidungsproblemen stehen mehrere Ziele im Konflikt zueinander und müssen einen gemeinsamen Nutzen bilden.“[42] Hier kann der Entscheidungsträger mittels Bewertung der Zielbeiträge der einzelnen Handlungsalternativen die für ihn vorteilhafteste Entscheidung treffen.[43] Dabei ist es äußerst wichtig, nach dem Prinzip der Zielneutralität zu handeln, denn nur so können unvoreingenommene, autonome Entscheidungen getroffen werden. Die Zielneutralität beschreibt hier die Unabhängigkeit bei Entscheidungen, d.h. es liegen keine Präferenzen zu den Handlungsalternativen vor.

4.3 Schilderung der Funktionsweise einer Nutzwertanalyse

Die Nutzwertanalyse (NWA) wird primär zur systematischen und transparenten Entscheidungsfindung bzw. zur Auswahl aus zwei oder mehreren Alternativen eingesetzt. Sekundär kann das Verfahren der Nutzwertanalyse zur Sortierung bzw. Priorisierung von Alternativen verwendet werden, womit jeder

---

[41] Vgl. (Jacob, 2012).

[42] Vgl. (Fleßa, 2015).

[43] Vgl. (Jacob, 2012).

Wahlmöglichkeit ein individueller Nutzwert zugeordnet wird. Die NWA behandelt infolgedessen mehrdimensionale Entscheidungsprobleme unter Sicherheit. Typische Anwendungsgebiete bzw. Fragestellungen in der Praxis wären z.B.:

- Auswahl eines Produktionsstandortes.
- Priorisierung der Einführung von Artikeln / Produkten.
- Welche Maschine passt am Besten in mein Fertigungsumfeld?

4.3.1 Die Vorgehensweise bei der Nutzwertanalyse

Die Entscheidungsfindung aus mehreren Alternativen mit Hilfe einer Nutzwertanalyse kann in sieben Schritte gegliedert werden. Ziel ist es den Nutzwert pro Alternative zu berechnen und jene Alternative mit dem höchsten Nutzwert, ist anschließend als „optimal" anzusehen. „Ein Nutzwert ist ein objektiver Wert, als Maß einer bestimmten Funktionserfüllung."[44] Außerdem ergibt sich anhand der unterschiedlichen Nutzwerte eine Priorisierung der Handlungsalternativen. Nach Kühnapfel ist als erstes das Arbeitsumfeld zu organisieren, um nachfolgend das eigentliche Entscheidungsproblem gemeinsam zu beschreiben, damit alle Beteiligten am selben Wissensstand sind. Im nächsten Schritt werden Problemlösungen bzw. Entscheidungsalternativen erarbeitet, welche dann anhand relevanter Entscheidungskriterien spezifiziert werden. Die Anzahl an Kriterien kann dabei beliebig groß sein. Die Handlungsalternativen und ihre Kriterien werden dann in eine Zielertragsmatrix transformiert (siehe Abbildung 5 & 6). Da bei der Auswahl zwischen mehreren Alternativen in der Regel wichtigere und weniger wichtige Entscheidungskriterien vorliegen, können diese anschließend durch eine (meist prozentuale) Gewichtung priorisiert werden.

[44] (Gabler, 2016).

1	Organisation des Arbeitsumfelds	• Festlegung des Teilnehmerkreises. • Festlegung eines ausreichenden Zeitrahmens.
2	Benennung des Entscheidungs-problems	Ausführliche Beschreibung des Entscheidungsproblems, damit alle Beteiligten auf demselben Wissensstand sind. Warum ist diese Entscheidung wichtig?
3	Auswahl der Entscheidungsalternativen	• Ermittlung der zu behandelnden Alternativen in Absprache aller Beteiligten.
4	Sammlung von Entscheidungskriterien	• Anhand welcher Kriterien soll eine Entscheidung getroffen werden bzw. was ist für die Unternehmung wichtig bzw. relevant?
5	Gewichtung der Entscheidungskriterien	• In welchem Verhältnis stehen die ausgewählten Kriterien zueinander?
6	Nutzwertberechnung	• Berechnung der Nutzwerte einzelner Alternativen mittels ordinaler und / oder kardinaler Skala.
7	Dokumentation des Ergebnisses	Eine gute Dokumentation ist essentiell zur transparenten und verständlichen Kommunikation an die Stakeholder.

Tabelle 5: Vorgehensweise bei der Nutzwertanalyse[45]

Nach der Kriteriengewichtung erfolgt eine Skalierung innerhalb der Nutzwertberechnung zur Charakterisierung der Zielerreichung der jeweiligen Alternativen.

[45] Vgl. (Kühnapfel, 2014).

In der Praxis stehen vier Methoden bzw. Typen der Skalierung zur Verfügung:

- Nominalskala
- Ordinalskala
- Kardinalskala
- Verhältnisskala

Nachfolgend wird die Methodik der Ordinal- und Kardinalskala näher beschrieben.

4.3.2 Das Scoring-Modell auf Basis einer Ordinalskala

Durch den Einsatz einer ordinalen Skala können Alternativen im Gegensatz zur Nominalskala in eine Rangordnung gebracht werden. Um eine Rangordnung herstellen zu können, bedarf es dem Auszuführenden die Kompetenz zur Beurteilung der Handlungsalternativen: Welche Alternative erfüllt die Entscheidungskriterien besser, gleich oder schlechter als die zu vergleichende Alternative?

Es können jedoch keine Angaben gemacht werden, um wieviel (Abstand) Alternative 1 besser ist als Alternative 2 bei Entscheidungskriterium X. (qualitatives Bewertungsverfahren) In der Praxis werden ordinale Skalen z.B. zur Messung von Eruptionen oder Windstärken verwendet.

Ordinale Skalen können beispielsweise wie folgt dargestellt werden:

	SSD Performance	Lesbarkeit d. Bildschirms	Preis	Gewicht	Design
HP	Gut	Sehr Gut	Mittel	Hoch	Befriedigend
Lenovo	Sehr Gut	Gut	Hoch	Niedrig	Befriedigend
Samsung	Gut	Befriedigend	Niedrig	Niedrig	Gut

Abbildung 6: Zielertragsmatrix mit ordinalen Werten

Hier werden bestimmte Produktmerkmale durch verbale, qualitative Werte ausgedrückt z.B.:

- Niedrig, Mittel, Hoch, Sehr Hoch
- Schlecht, Befriedigend, Gut, Sehr Gut

Zur Berechnung des Nutzwertes (siehe 5.3.4) werden diese verbalen Werte mittels einer Skalentransformation in numerische Werte transformiert. So wird eine beliebige Skala mit einem relativen Nullpunkt und einem Endpunkt festgesetzt (ähnlich einem simplen Zahlenstrahl) z.B.: 0 -10:

Abbildung 7: Zahlenstrahl

Anschließend werden die qualitativen Aussagen an der numerischen Skala streng monoton gereiht z.B.:

- Sehr Gut = 10
- Gut = 7,5
- Mittel = 5
- Schlecht = 2,5
- Miserabel = 0

4.3.3 Die kardinale Skala als Grundlage der Nutzwertanalyse

Die Kardinalskala ist im Gegensatz zur Ordinalskala ein quantitatives Bewertungsverfahren, da hier nicht nur die Rangordnung der Handlungsalternativen bestimmt wird, sondern auch der quantitative, numerische Abstand zwischen den Wahlmöglichkeiten. Anhand der nachfolgenden Tabelle wird der Unterschied zu den ordinalen Wertungen (Design) verdeutlicht:

	SSD Performance	Bildschirmauflösung	Preis	Gewicht	Design
HP	400MB/s	320dpi	2.100 €	2850g	Befriedigend
Lenovo	500MB/s	280dpi	2.689 €	1200g	Befriedigend
Samsung	420MB/s	235dpi	1.699 €	1280g	Gut

Abbildung 8: Zielertragsmatrix mit ordinale und kardinale Werten

Am obigen Beispiel lässt sich im Gegensatz zum Kriterium „Design“ bei allen anderen Kriterien exakt feststellen, um wieviel besser / schlechter Alternative A als Alternative B ist. (Samsung Notebook wiegt 80g mehr als das Lenovo). Die quantitativen Werte müssen zur Berechnung des Nutzwertes ebenfalls wie bei der Ordinalskala noch in vergleichbare Werte transformiert werden. Dazu wird der beste (nicht zwangsläufig höchste Wert -> Preis) als höchster Wert im gewählten Skalenniveau gesetzt z.B.:

*Lenovo SSD Performance: 500MB/s entspricht auf einer Skala von 1-10 dem Wert **10**.*

Anschließend wird mittels einer simplen Schlussrechnung der Wert für die Samsung SSD berechnet: *(420*10)/500=**8,4***

4.3.4 Die Berechnung des Nutzwertes anhand der Nutzwertanalyse

Sind die Schritte 1-5 der NWA erledigt, folgt die eigentliche Berechnung des Nutzwertes. Der Nutzwert kann als ein Maß beschrieben werden, wie sehr ein Gut / eine Alternative hinsichtlich festgelegter Kriterien / Präferenzen für eine Unternehmung geeignet ist.

	SSD Performance	Bildschirmauflösung	Preis	Gewicht	Design
HP	400MB/s	320dpi	2.100 €	2850g	Befriedigend
Lenovo	500MB/s	280dpi	2.689 €	1200g	Befriedigend
Samsung	420MB/s	235dpi	1.699 €	1280g	Gut

Abbildung 9: Zielertragsmatrix für die Transformation in eine Zielwertmatrix

Auf Basis der Zielertragsmatrix aus dem vorherigen Beispiel werden die Werte durch eine Wertsynthese in eine Zielwertmatrix transformiert. Dabei

werden die Beurteilungen (B) mit den zuvor definierten Gewichten (G) multipliziert, um die Teilnutzwerte pro Entscheidungskriterium zu erhalten:

Kriterien	G	Maßnahmen					
		HP		*Lenovo*		*Samsung*	
		B	**TNW**	**B**	**TNW**	**B**	**TNW**
SSD Performance	30%	8	2,4	10	3	8,4	2,52
Bildschirmauflösung	20%	10	2	8,75	1,75	7,34	1,468
Preis	15%	8,09	1,2135	6,32	0,948	10	1,5
Gewicht	25%	4,21	1,0525	10	2,5	9,37	2,3425
Design	10%	5	0,5	5	0,5	7,5	0,75
Nutzwertsumme			**7,166**		**8,698**		**8,581**

Tabelle 6: Berechnung des Nutzwertes mittels NWA

Abschließend werden alle Teilnutzwerte je Alternative summiert um den Gesamtnutzwert zu erhalten. Da die Alternative „Lenovo“ die höchste Nutzwertsumme aufweisen kann, ist diese als optimal anzusehen.

4.4 Das Prinzip des Goal-Programmings erläutert

Bei der Goal-Programmierung oder auch Satifizierungsregel genannt, sollen fixierte Ziele möglichst genau erreicht werden, wobei die Abweichungen nach oben und unten zu minimieren sind.[46] Somit lässt sich folgendes festhalten: „Optimale Aktion ist die mit der minimalen, absoluten Abweichungssumme von den Vorgabewerten (fiktive Aktion).“[47] Dies bedeutet auch, dass der Entscheidungsträger über eine entsprechende Vorstellung der gewünschten bzw. realisierbaren Ziele, je Entscheidungskriterium verfügen muss. In anderen Worten

[46] Vgl. (Wirtschaftslexikon24, 2015).

[47] (Stelling, 2009).

ausgedrückt: Der Entscheidungsträger muss sich vor der Wertsynthese ausführlich Gedanken über die zu erstrebenden Ziele machen.

4.4.1 Die Vorgehensweise bei der Goal-Programmierung

„Zunächst wird für jedes Ziel, das mit einer Zuordnung erfüllt werden soll, ein Sollwert – ein so genanntes Goal – festgelegt, der an einem bestimmten Zuordnungsplatz angestrebt wird.“[48] Anschließend werden die Istwerte der Zielerreichung erfasst und in der Matrix eingetragen. Durch Subtraktion der Istwerte von den „Goals“ erhält man die Abweichung, welche möglichst gering sein sollte. Jede einzelne Abweichung zum Zielwert wird nachfolgend pro Aktion / Alternative miteinander addiert, woraus sich abschließend der Nutzen (N) pro Alternative ergibt. Sollte der Wert aus der Zielwertmatrix größer als das gesetzte Ziel sein, so ist das Goal vom eingetragenen Wert abzuziehen. Jene Aktion mit dem geringsten Nutzen (geringste Summe der Abweichungen) ist nun zu wählen.

4.4.2 Das Goal-Programming empirisch veranschaulicht

Als Ausgangssituation stehen drei Alternativen (A_1, A_2, A_3) mit jeweils vier Entscheidungsparameter (P_1, P_2, P_3, P_4) zur Verfügung.

- Die Parameter sind für die Wertsynthese wie folgt festgelegt:

  P_1= 8, P_2=7, P_3=9, P_4=9

- Die Zielwertmatrix liegt bereits vor (B=Beurteilung).

[48] (Zelewski, et al., 2005).

Kriterien	Goals	Alternativen		
		A_1	A_2	A_3
		B	B	B
P_1	8	6,5	7	7,5
P_2	7	8	6	7
P_3	9	10	8,5	9
P_4	9	9	9	10
Zielerreichnung		**3,5**	**2,5**	**1,5**

Tabelle 7: Zielwertmatrix für die Goal-Programmierung

Beispiel A_1:

N= (8-6,5)+(8-7)+(10-9)+(9-9) => ***3,5***

Da A_3 in Summe die geringste Abweichung zu den zuvor definierten Zielen hat, ist Alternative 3 zu wählen.

4.5 Die Sicherheitsziele im IT-Risikomanagement im Einklang zur Unternehmensstrategie

„Die Kunst der IT-Sicherheit besteht darin, die Gefährdungen, denen die IT-Systeme und Daten ausgesetzt sind, möglichst aus den verschiedensten Perspektiven zu betrachten und dann diejenigen Maßnahmen auszuwählen, die unter der Berücksichtigung von Kosten und Nutzen den meisten Erfolg im Zusammenspiel versprechen.“[49] Um diesen Erfolg erzielen zu können, ist es wichtig, sicherheitsrelevante Ziele / Objectives zu definieren, welche den Leitfaden bei der nachfolgenden Business Impact Analyse und der Risikoanalyse mittels Audit bilden. Diese Sicherheitsziele sollten individuell auf das bestehende Geschäftsfeld und die Unternehmensstrategie angepasst werden.

[49] (Harich, 2015).

Nachfolgend werden einige mögliche Sicherheitsziele gelistet, welche immer für alle IT-Prinzipien gelten zu haben:

Sicherheitsziele		
VERTRAULICHKEIT	**INTEGRITÄT**	**VERFÜGBARKEIT**
1- Unterbindung von Beeinträchtigungen im Datenschutz		
2- Unterbindung von Rechtsverstößen		
3- Unterbindung des Verletzens von Regeln und Vorschriften		
4- Unterbindung von Vertragsverstößen		
5- Unterbindung von Beeinträchtigungen bei Geschäftsprozessen		
6- Unterbindung von negative, externen Effekten		
7- Das Verhindern eines Wettbewerbsnachteils und möglichen Schäden an immateriellen Vermögenswerten		
8- Sicherstellung der persönlichen Sicherheit		
9- Unterbindung von negativen, finanziellen Konsequenzen		

Tabelle 8: Sicherheitskriterien [NTT Com Security]

5 Das Zusammenspiel von Entscheidungstheorie und Risikomanagement

Im folgenden Kapitel soll der theoretisch behandelte Risikomanagementprozess empirisch an einem Beispiel umgesetzt werden und als Meta-Prozess im operativen Risikomanagement fungieren. Die einzelnen Prozessphasen werden mit Hilfe von international standardisierten und bewährten Methoden unterstützt bzw. umgesetzt. Die zentrale Darstellung des Risikos mittels Risikoerwartungswert (R=I*L) bleibt unangetastet und wird zur weiteren Erörterung als feste Konstante gesehen. Die prozessunterstützenden Tools werden anschaulich hinsichtlich ihrer Funktionsweise, wie etwa die Business Impact Analyse, zur Identifikation der Auswirkungen erörtert und die Zusammenhänge zwischen den Prozessphasen empirisch repräsentiert. Weiter soll die Beziehung zwischen der Eintrittswahrscheinlichkeit und den Ergebnissen aus der Risikoanalyse verdeutlicht werden – auf diese Weise wird auch die Bewertung und Kategorisierung der Risiken in der Praxis ersichtlich. Anschließend wird durch die Anwendung der Instrumente „Nutzwertanalyse“ und „Goal-Programming“ aus dem Gebiet der Entscheidungstheorie der Entschluss, welche Gegenmaßnahmen getroffen werden, dargelegt. Außerdem werden die Nutzwertanalyse und das Goal-Programming gegenübergestellt, miteinander verglichen und jeweilige Vor- und Nachteile eruiert.

5.1 Die Business Impact Analyse zur Identifikation der Auswirkungen auf IT Services

Eingehend soll die Vorgehensweise und die Funktionalität einer Business Impact Analyse beschrieben werden. Die Business Impact Analyse (BIA) zählt zu den gängigsten Methoden im IT-Sicherheitsmanagement, um Auswirkungen auf IT-relevante Prozesse, Services oder Applikationen zu identifizieren. Weiter wird die BIA für das Ermitteln von kritischen Geschäftsprozessen und

Ressourcen für den Wiederanlauf nach Unterbrechungen verwendet.[50] „Unter dem Aspekt der Wirtschaftlichkeit muss herausgefunden werden, wie unternehmenskritisch die erbrachten Leistungen oder Produkte und die hierzu erforderlichen Geschäftsprozesse sind, um sie dementsprechend abzusichern, Schwerpunkte setzen zu können und sich auf das Wesentliche zu konzentrieren.“[51] „Da die Eintrittswahrscheinlichkeit von Ereignissen jedoch meist retrospektiv ist und Ereignisse erstmals oder trotz äußerst geringer Eintrittswahrscheinlichkeit sehr zeitnah auftreten können, hilft die BIA, den Blick auf den Schutzbedarf und die Folgen eines Ausfalls zu richten – unabhängig von der konkreten Ursache.“[52]

Durch die Ermittlung der Auswirkungen auf IT Services, kann also der Schutzbedarf je Service, bezogen auf die drei IT-Prinzipien, bestimmt werden. Der Schutzbedarf wird für die anschließende Risikoanalyse benötigt.

Die BIA zählt beim Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Basis im Notfallmanagement. Nach BSI bedarf es einer vorrangigen Business-Impact-Analyse, damit eine nachrangige Risikoanalyse durchgeführt werden kann. „Zusammen mit der Risikoanalyse bildet die BIA die Grundlage für eine effektive Sicherheits- und Notfallvorsorgestrategie und die Basis für das Notfallvorsorgekonzept.“[53]

[50] Vgl. (BSI, 2015).

[51] (Hämmerle, 2016).

[52] Ebd.

[53] (Reiss, et al., 2014).

5.1.1 Die Komponenten einer Business Impact Analyse

Die BIA kann wie folgt in drei Segmente gegliedert werden:

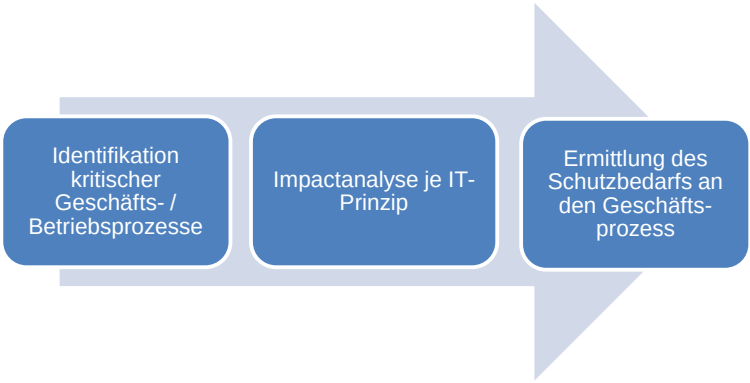

Abbildung 10: Komponenten einer Business-Impact-Analyse [eigene Darstellung]

Nachfolgend sollen die einzelnen Komponenten der Business Impact Analyse am Beispiel einer Handelskette erläutert werden.

5.1.2 Identifikation kritischer Geschäfts- und Betriebsprozesse

Geschäftsprozesse werden beschleunigt, automatisiert und virtualisiert, weshalb komplexe Steuerungs-, Kontroll- und Informationssysteme zur Datenverarbeitung / Datensicherung erforderlich sind und von Spezialisten-Teams betreut werden.[54] Je nach Geschäftsfeld des Unternehmens sind diese Prozesse individuell zu identifizieren, da z.B. ein Produktionsbetrieb andere Abläufe in Verwendung hat, als eine Handelskette und somit auch unterschiedliche Prioritäten der internen Geschäftsfunktionen setzt. Ein Ausfall ertragswichtiger Komponenten muss möglichst rasch wiederhergestellt werden, um nicht finanzielle Verluste zu vermeiden. „Die Geschäftsprozesse mit der

[54] Vgl. (Read, 2016).

höchsten Priorität der Wiederaufnahme bezeichnet man als „Mission Critical Activities“ oder als kritische Geschäftsfunktionen.“[55]

Zur Identifikation der kritischen Geschäftsfunktionen müssen nach Read zentrale Fragestellungen behandelt werden:[56]

- *Was passiert wenn Prozess A ausfällt?*
- *Wo muss angegriffen werden, damit mit dem kleinsten Aufwand die größten negativen Wirkungen erreicht werden?*
- *Welche Auswirkungen hat ein Ausfall von Prozess A?*
- *Was muss funktionieren, damit Prozess A nicht ausfällt?*

Beispiel Handelskette:

Eine Handelskette erwirtschaftet ihren Umsatz durch den direkten Verkauf von Waren am Verkaufsort (Point of Sale). Der Verkauf spiegelt darüber hinaus einen IT-Service im Unternehmen wider, da alle für den Verkauf notwendigen IT-Komponenten, einem Service (z.B.: Retail) zugeordnet sind. Ist der Verkaufsprozess nicht mehr möglich, so ist für die Gesellschaft ein massiver Schaden zu erwarten, weshalb dieser Prozess unter den „Mission Critical Activities“ einzuordnen ist.

[55] (Ulrich, 2010).

[56] Vgl. (Read, 2016).

5.1.3 Die Analyse der Auswirkungen auf die Sicherheitsziele

Im Abschnitt 5.5 wurde auf die Notwendigkeit definierter Sicherheitsziele im Unternehmen für die Business Impact Analyse hingewiesen. Im zweiten Teil der BIA werden nun die Auswirkungen auf die betrieblichen Sicherheitsziele je IT-Prinzip untersucht. Dabei wird jedes Schadensausmaß anhand einer Identifikation (BI-ID) gekennzeichnet und einem IT-Prinzip zugeordnet:

$A_1 \ldots A_n$ = *Availability Impacts*
$C_1 \ldots C_n$ = *Confidentiality Impacts*
$I_1 \ldots I_n$ = *Integrity Impacts*

Die Klassifizierung der Auswirkung je Sicherheitsziel wird durch eine knappe, aussagekräftige Beschreibung ergänzt. In der Regel wird eine Skala von 0-4 verwendet:

0 – Nicht Adressierbar
1 – Niedrig
2 – Mittel
3 – Hoch
4 – Sehr Hoch

Die jeweils höchste Bewertung eines Sicherheitszieles ergibt die Gesamtauswirkung auf den IT-Service bezogen auf die Grundwerte (CIA[57]).

Die Impact-Analysen hinsichtlich der Dimensionen Integrität und Vertraulichkeit sind unter den Anlagen Teil 1 & 2 zu finden.

[57] Confidentiality, Integrity & Availability.

Beispiel Handelskette & Retail-Service:

Business Impact Availability: Retail-Service			**3 - High**
BI-ID	**Sicherheitsziele**	**Description**	**Impact**
A-1	Impairment of data privacy	*Data privacy is not impaired in case the application is not available. There is little to no negative impact on data privacy in case of an application outage.*	1- Low
A-2	Legal Breaches	*A business impact due to legal breaches from unavailability is considered low as the function of registrating sales (Registrierkassenpflicht) can be executed offline. Sales can still take place.*	1- Low
A-3	Breaches of rules and regulations	*Even though not formalized, internal regulations insist on high availability of application as sales data is very important and needs to be available on a daily basis.*	3- High
A-4	Breach of contracts	*Breach of contracts is not applicable as partner stores do not exist in Austria.*	0- n/a
A-5	Impairment of business processes	*A high impact on business processes is expected in case of non- availability due to additional work and possible overtime of employees to add missing data from application outage back into the system. Also, the reporting system will be delayed due to missing data from database.*	3- High
A-6	Negative external effects	*Negative external effects from non- availability can be disgruntled customers as they have to spend more time at the POS.*	2- Medium
A-7	Competitive disadvantage and intangible damage	*Dissatisfied customers might turn to competitors and buy there.*	3- High
A-8	Personal safety	*not applicable*	0- n/a
A-9	Financial consequences	*Sales might decline in case customers prefer to buy at competitor.*	2- Medium

5.1.4 Ermittlung des Schutzbedarfs an den IT-Service

Im dritten und letzten Schritt der BIA wird der Schutzbedarf an dem identifizierten Geschäftsprozess / Service je IT-Prinzip (Verfügbarkeit, Integrität und Vertraulichkeit) erhoben. Diese Anforderungen werden gewöhnlich wiederum in vier ordinale Werte bzw. Schutzbedarfsklassen (sehr hoch, hoch, mittel, gering) gestuft.

Dabei spiegeln die Impactwerte (aus Schritt 2) den Schutzbedarf des Services wider. Ein hoher Business-Impact auf die Verfügbarkeit eines Services fordert folglich einen hohen Schutzbedarf an die Verfügbarkeit.

Zweck dieser Klassifizierung ist die Ermittlung der dahinterliegenden Anforderungen an die Systemlandschaft des Geschäftsprozesses bzw. Services.

Schutzbedarf Verfügbarkeit [Retail Service]		
Wert	**SBK[58]**	**Anforderung / Beschreibung**
4	4- Sehr Hoch	Daten müssen kontinuierlich verarbeitet werden. Massive bzw. existenzbedrohende Schäden werden bei einer Nicht-Verfügbarkeit von über vier Stunden erwartet.
3	3- Hoch	Die Nicht-Verfügbarkeit von Daten wird lediglich einen Tag toleriert, ansonsten ist ein hoher Schaden zu erwarten.
2	2- Mittel	Die Nicht-Verfügbarkeit von Daten wird bis zu einer Woche toleriert. Manuelle Fall-Back-Szenarien verhindern hohe Schäden.
1	1- Niedrig	Die Verarbeitung von Daten kann sich bis zu zehn Wochen verspäten. Innerhalb dieser Zeit können manuelle Fall-Back-Szenarien merkbare Schäden verhindern.

Tabelle 9: Beispiel Schutzbedarf Verfügbarkeit

[58] SBK…Schutzbedarfsklasse.

Schutzbedarf Vertraulichkeit [Retail Service]		
Wert	**SBK**	**Beschreibung**
4	4- Sehr Hoch	Unbefugte Weitergabe von Daten kann zu schweren Schäden führen, Vorteile für einen Mitbewerber bringen oder hat schwerwiegende Auswirkungen auf die Geschäftseinheit.
3	3- Hoch	Unbefugte Weitergabe von Daten kann die Geschäftseinheit nachteilig beeinflussen.
2	2- Mittel	Unbefugte Weitergabe von Daten würde zu keine erheblichen Schäden der Geschäftseinheit führen.
1	1- Niedrig	Die Weitergabe von Daten an die Öffentlichkeit oder 3rd Party Betriebe stellt kein Risiko dar.

Tabelle 10: Beispiel Schutzbedarf Vertraulichkeit

Schutzbedarf Integrität [Retail Service]		
Wert	**SBK**	**Beschreibung**
4	4- Sehr Hoch	Beabsichtigte und unbeabsichtigte Beschädigung von verarbeiteten Daten kann zu massiven Schäden führen. Nicht-reproduzierbare Daten verursachen in der Regel hohe Schäden. Ihre Wiederherstellung sollte lediglich zwischen 0 und vier Stunden betragen.
3	3- Hoch	Beabsichtigte und unbeabsichtigte Beschädigung von verarbeiteten Daten kann zu hohen Schäden führen. Nicht-reproduzierbare Daten verursachen in der Regel hohe Schäden. (Gehaltsdaten, Jahresabschluss, Produktdaten). Ihre Wiederherstellung sollte zwischen vier und 24 Stunden betragen.
2	2- Mittel	Beabsichtigte und unbeabsichtigte Beschädigung von verarbeiteten Daten kann zu mittleren Schäden führen. Nicht-reproduzierbare Daten verursachen in der Regel mittlere Schäden. (publizierte Managemententscheidungen). Ihre Wiederherstellung sollte zwischen 24 Stunden und einer Woche betragen.
1	1- Niedrig	Beabsichtigte und unbeabsichtigte Beschädigung von verarbeiteten Daten haben keinen negativen Effekt. Die Daten müssen nicht für 3rd Parties wiederhergestellt werden. Ihre Wiederherstellung beantragt kann in jedem Falle über einer Woche betragen.

Tabelle 11: Beispiel Schutzbedarf Integrität

Zusammenfassend lässt sich festhalten, dass mit Hilfe der Business Impact Analyse der erste Faktor zur Bemessung des Risikoerwartungswertes erarbeitet wurde:

Risikoerwartungswert = ***Auswirkung*** * *Eintrittswahrscheinlichkeit*

Im nächsten Schritt wird die Risikoanalyse mittels ISO 27002 Audit veranschaulicht, um anschließend die Eintrittswahrscheinlichkeit bestimmen zu können.

5.2 Der ISO 27001 Audit als Basis der Risikoanalyse

Die Risikoanalyse ist ebenso wie die Business-Impact-Analyse, Teil der praktischen Umsetzung des Risikomanagementprozesses. Das Ziel der Risikoanalyse besteht darin, Risiken zu identifizieren und zu bewerten. Grundlegend ist es immer sinnvoll, international akzeptierte gute Vorgehensmodelle als Basis zu verwenden, was in der IT-Sicherheit eine Reihe von ISO-Standards darstellt.[59] Diese Standards sind Teil des ISMS (Information Security Management System), welches dazu dient, die Sicherheit in der Informationstechnologie zu gewährleisten und aufrechtzuerhalten. Der bereits erwähnte IT-Grundschutz nach BSI ist unter anderem ein Entwurf solch eines ISMS für kleine und mittelständige Unternehmen. Für international tätige Großunternehmen ist dieser IT-Grundschutz meist nicht ausreichend. Risikoanalysen in Großunternehmen sind in der Regel sehr aufwändig und komplex, weshalb hier gewöhnlich ein Audit nach ISO 27001 als Basis verwendet wird. „Wichtige Zielsetzungen von ISO/IEC 27001 sind die Festlegung einer einheitlichen Terminologie und die Definition einheitlicher (standardisierter) Kriterien, nach denen Organisationen hinsichtlich einer umfassenden und effektiven Verwaltung und Steuerung ihrer Aktivitäten zur Gewährleistung der Informationssicherheit

[59] Vgl. (Harich, 2015).

bewertet (auditiert) werden können.“[60] Aus diesem Grunde soll auch der Ablauf eines Audits nach ISO 27001 knapp dargelegt werden, da diese Vorgehensweise zunehmend Bedeutung in Unternehmen findet.

5.2.1 Identifikation von Abweichungen zur ISO 27001

In der ISO/IEC 27001 werden Risiken anhand von Abweichungen zur Norm bestimmt. Abweichungen werden in der Informationstechnologie als sogenannte GAPs bezeichnet. Sie beschreiben die Abweichung eines Ist-Zustandes zu einem definierten Soll-Zustand.

Beispiel GAP:

Die Passwortpolicy beinhaltet nicht die aktuell notwendige Komplexität eines Passwortes. Es werden lediglich acht von zehn erforderlichen Zeichen gefordert.

Die Norm gibt dabei den Soll-Zustand bzw. Vorgaben zu bestimmten Unternehmensbereichen vor. Diese Vorgaben werden „Controls“ genannt, welche in Gruppen gegliedert sind. Insgesamt sind in der ISO/IEC 27001:2013 114 Controls innerhalb 14 gekennzeichneten (A.xx) Gruppen gelistet. Die Bedingungen sind im Zuge des Audits für das jeweilige Unternehmen auf Relevanz zu prüfen und gegebenenfalls anzupassen. Dabei werden jedoch keine Controls geändert, sondern irrelevante Themen nicht behandelt oder einzelne Controls ausgelassen. Gruppen eines ISO-Audits sind:

A.5	Security policy	Sicherheitsrichtlinien
A.6	Organization of information security	Organisation der Informationssicherheit
A.7	Human resource security	Personalsicherheit
A.8	Asset Management	Asset Management
A.9	Access control	Zugriffskontrolle
A.10	Cryptography	Kryptografie
A.11	Physical and environmental security	Physikalische und Umweltsicherheit
A.12	Operations security	Betriebssicherheit

[60] (MITSM, 2016).

A.13	Communications security	Kommunikationssicherheit
A.14	System acquisition, development and maintenance	Systembeschaffung, Entwicklung und Wartung
A.15	Supplier relationships	Lieferantenbeziehungen
A.16	Incident Management	Problemmanagement
A.17	Information security aspects of business continuity management	Aspekte der Informationssicherheit an d. betriebliche Kontinuitätsmanagement
A.18	Compliance	Regelkonformität

Tabelle 12: Gruppen des ISO 27001 Audits[61] [eigene Darstellung]

Zum Erhalt einer Zertifizierung nach ISO/IEC 27001:2013 sind die Anforderungen aus den 114 Controls in einem bestimmten Maß zu erfüllen. Eine Zertifizierung ist jedoch nicht für jedes Unternehmen von Interesse, sondern vielmehr lässt sich mit Hilfe des Grades an Übereinstimmung mit der Norm, ein Überblick über die aktuelle Sicherheitslage der eigenen Unternehmenslandschaft verschaffen. Wie sehr der aktuelle Ist-Zustand die Vorgaben aus der ISO 27001 erfüllt, wird in der Regel mit Hilfe eines Reifegrades ermittelt. Der Reifegrad beschreibt einen quantitativen Abstand zur Norm im Gegensatz zu einem GAP, welcher die konkrete Abweichung in Worten beschreibt. Mit Hilfe eines Reifegrades lässt sich auf den ersten Blick bestimmen, wie gut z.B. ein Prozess im Unternehmen etabliert ist. Dies ist insofern wichtig, da die ISO 27001 ähnlich dem Risikomanagementprozess auf dem Gedanken der kontinuierlichen Verbesserungsstrategie aufbaut ist.

Es ist empfehlenswert die Erhebung des IST-Zustandes von einem externen Auditor durchzuführen, um das Prinzip der Unvoreingenommenheit wahren zu können. Unternehmensinterne Personen neigen nämlich ihr persönliches Verantwortungsgebiet besser darzustellen als es wirklich ist. Nachfolgend ist ein kleiner Ausschnitt eines möglichen Audits dargestellt.

[61] Vgl. ISO 27001.

ID	Gruppen	Controls ISO 27001 (unternehmensspezifisch)	Vorgabedetails	BIA	Relevant?
A 17.1.1	Aspekte der Informationssicherheit an d. betriebliche Kontinuitätsmanagement	Strategie um die Betriebskontinuität zu gewährleisten.	Je nach den Ergebnissen aus der BIA, hat ein Konzept für die Hochverfügbarkeit vorzuliegen.	**3**	Ja
A 10.1.1.b	Kryptografie	Typ, Stärke und Qualität der Verschlüsselung.	Das notwendige Schutzniveau unter Berücksichtigung der Art, Stärke und Qualität des Verschlüsselungsalgorithmus ist festgelegt und dokumentiert.	**3**	Ja
A 12.1.1.a	Betriebssicherheit	Verarbeitung und Handhabung von Informationen.	Ausführliche Anweisungen für die Verarbeitung und Handhabung von Daten müssen dokumentiert sein.	**3**	Ja

Tabelle 13: Anforderungen der ISO 27001 inkl. BIA aus 6.1.4

Die im Abschnitt 6.1.4 ermittelten Schutzbedarfsklassen aus der BIA werden hier ebenfalls, passend zu den jeweiligen Gruppen, eingetragen:

***A17**... Business Impact Availability*

***A10**… Business Impact Vertraulichkeit*

***A12**… Business Impact Integrität*

Sie spiegeln den erforderlichen Reifegrad aus der ISO 27001 wider, welcher wiederum die Vorgaben an die Controls spezifiziert. Nachdem der Soll-Zustand mit den Ergebnissen aus der BIA erweitert wurde, gilt es, den Ist-Zustand zu ermitteln. Hierzu wird der Ist-Zustand in der Regel durch den externen Auditor in Form eines Interviews analysiert und knapp im Audit Protokoll vermerkt. Der Auditor bewertet im Anschluss den aktuellen Reifegrad auf Basis des IST-Zustandes.

Implementierung der Vorgabe		Reifegrad	
Beschreibung des Ist-Zustands	**Spezifikation der Quelle**	**erforderlich**	**aktuell**
Die Serverinfrastruktur ist zwar redundant ausgelegt, jedoch befinden sich alle Server in nur einem Rechenzentrum.	Interview mit dem Sicherheitsverantwortlichen am xx.xx.xx	3	1
kryptographische Algorithmen, Verschlüsselungen, Schlüsselaustausch und digitale Signaturen sind festgelegt und dokumentiert	Interview mit dem Sicherheitsverantwortlichen am xx.xx.xx	3	3
Richtlinien für die Verarbeitung und Handhabung von Daten sind implementiert und werden regelmäßig überarbeitet	Interview mit dem Sicherheitsverantwortlichen am xx.xx.xx	3	4

Tabelle 14: Ist-Zustand inkl. Reifegrad

Diese Vorgehensweise ist für alle relevanten Anforderungen durchzuführen, was den zeitlichen Aufwand eines solchen Audits verdeutlicht und auch begründet, warum der ISO 27001 Audit zur Risikoanalyse in der Regel nur bei Großunternehmen Anwendung findet.

Nachdem alle relevanten Gruppen und Controls des Audits behandelt worden sind, wird die Durchschnittswertung aller Controls je Gruppe für den Soll- und den Ist-Zustand ermittelt:

Chapter	Title	Ø Target	Ø Actual
A.5	Security policy	3,0	2,3
A.6	Organization of information security	2,9	2,6
A.7	Human resource security	3,0	3,0
A.9	Access control	3,0	2,8
A.10	Cryptography	3,0	2,0
A.12	Operations security	2,8	1,2
A.13	Communications security	3,0	2,5
A.16	Incident Management	3,0	2,9
A.17	Information security aspects of business continuity management	2,7	1,1
A.18	Compliance	2,9	2,0

Tabelle 15: Übersicht der Bewertungen eines ISO 27001 Audits

Zur besseren Veranschaulichung lassen sich diese Werte in einem Spinnendiagramm wie folgt darstellen:

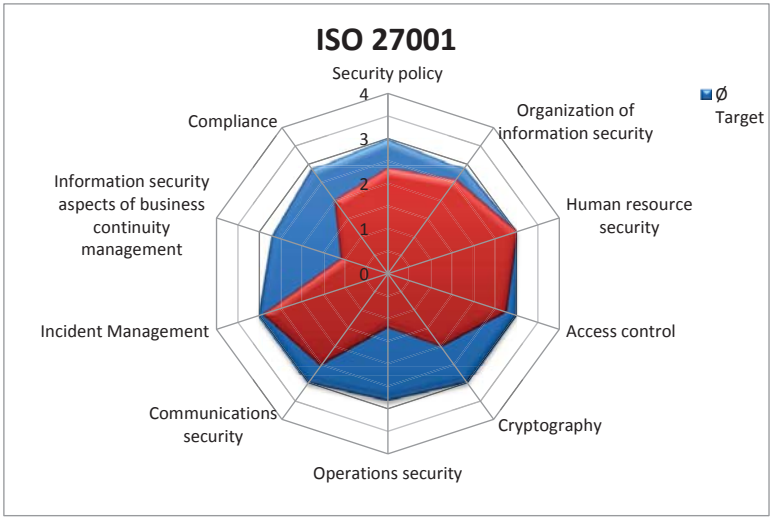

Abbildung 11: Spinnendiagramm eines ISO 27001 Audits

Es ist ersichtlich, dass in den Bereichen Betriebssicherheit, betriebliches Kontinuitätsmanagement und Kryptographie die größten GAPs bzw. geringsten Reifegrade vorliegen. Zur weiteren Ursachenbehebung werden anschließend jene Controls mit den größten Abweichungen herangezogen.

5.2.2 Der Zusammenhang zwischen Eintrittswahrscheinlichkeit und den Ergebnissen aus der Risikoanalyse

Der Begriff „Eintrittswahrscheinlichkeit“ wurde bereits im Abschnitt 3.1. erläutert, weshalb nachfolgend besonders auf den Zusammenhang zu den Ergebnissen aus der Risikoanalyse eingegangen wird. Im Zuge des ISO 27001 Audits wurden Abweichungen zu den erforderlichen Schutzbedarfsklassen aus der BIA und den Anforderungen aus der Norm, in Form eines Reifegrades, identifiziert.

Wie lässt sich nun eine Relation zwischen Reifegrad und der Eintrittswahrscheinlichkeit eines Risikos herstellen?

Es gilt folgende Annahme:

Die ISO/IEC 27001 ist Teil eines ISMS und hat infolgedessen das Ziel einer bestmöglichen Gewährleistung der Informationssicherheit (siehe 6.2). Weiter stellt sie unterschiedliche Ansprüche an den jeweiligen Reifegrad eines Controls. Ein höherer Reifegrad bedeutet höhere Anforderungen an dessen Informationssicherheit.

Es kann folgende These aufgestellt werden:

Je höher der Reifegrad eines Controls, desto stärkere Schutzmaßnahmen sind bereits implementiert. Je stärker die Schutzmaßnahmen, desto geringer ist folglich die Wahrscheinlichkeit eines erfolgreichen Angriffs.

Auf Basis dieser These kann eine Risikomatrix –ähnlich 4.4.1 - aufgestellt werden, welche die Wahrscheinlichkeit und die zu erwartende Auswirkung zur Ermittlung des Risikoerwartungswertes gegenüberstellt:

Wahrscheinlichkeit	Auswirkung/Schaden			
	Niedrig	Mittel	Hoch	Sehr hoch
Sehr wahrscheinlich	gering	mittel	hoch	sehr hoch
Wahrscheinlich	gering	mittel	hoch	hoch
Möglich	gering	gering	mittel	mittel
Unwahrscheinlich	gering	gering	gering	gering

Tabelle 16: Risikomatrix [eigene Darstellung]

Die Wahrscheinlichkeit wird nach BSI in vier Stufen gegliedert[62]:

- „sehr wahrscheinlich“: einmal pro Woche oder öfter,
- „wahrscheinlich“: einmal pro Monat,
- „möglich“: einmal pro Jahr,
- „unwahrscheinlich“: alle 10 Jahre oder seltener.

Das Risiko kann mittels Risikomatrix qualitativ beurteilt werden oder durch Transformation der qualitativen Aussagen in Zahlenwerte berechnet werden:

- „sehr wahrscheinlich“……..**4**……Reifegrad 1
- „wahrscheinlich“……**3**……Reifegrad 2
- „möglich“……**2**……...Reifegrad 3
- „unwahrscheinlich“……**1**……Reifegrad 4

Beispiel; Berechnung des Risikoerwartungswertes:

Risikoerwartungswert **R** für das betriebliche Kontinuitätsmanagement **A17**:

Reifegrad=1,1 -> Wahrscheinlichkeit= 3,64

Wahrscheinlichkeitsberechnung mittels Dreisatz: ((4*1)/1,1)~**3,64**

R=I*L -> 3,64*3=**10,92**

Skala des Risikoerwartungswertes:

12 < R……..…Risiko ist sehr hoch

8 < R ≤ 12……..Risiko ist hoch

4 < R ≤ 8……Risiko ist mittel

R ≤ 4……..……Risiko ist gering

[62] (BSI, 2016).

5.3 Maßnahmenentscheidung mittels Nutzwertanalyse und Goal-Programming im direkten Vergleich

Im Abschnitt 6.2 wurde die Identifikation und Bewertung von Risiken im Zuge einer Risikoanalyse veranschaulicht. Der letzte Teil dieses Kapitels ist der Maßnahmenentscheidung gewidmet, welche Teil der Risikosteuerung im Risikomanagementprozess ist. Um Risiken entgegenzuwirken, bedarf es der Implementierung von Gegenmaßnahmen im Einklang zur gewählten Risikostrategie.

Doch welche Maßnahme bringt den meisten Nutzen? Und wie lassen sich Entscheidungen transparent nach Außen vermitteln?

Diese Fragen sind häufig nicht einfach zu beantworten, weshalb in diesem Teil die bereits theoretisch behandelten Instrumente der Entscheidungstheorie, Hilfestellungen bieten sollen. In diesem Zuge werden Nutzwertanalyse und Zielprogrammierung an einem Beispiel miteinander verglichen, um im letzten Kapitel die Ergebnisse der Arbeit darzulegen.

Folgendes Beispiel dient als Basis für die Maßnahmenentscheidung:

Im Abschnitt 6.2.1 wurde im Zuge der Risikoanalyse, ein nicht unwesentlicher Handlungsbedarf bei Control A17.1.1 im Bereich der Hochverfügbarkeit, identifiziert. Die Analyse des Ist-Zustandes hat ergeben, dass sich die gesamte Serverinfrastruktur in einem einzelnen Rechenzentrum befindet. Der Schutzbedarf des Retail-Services an die Verfügbarkeit der Systemlandschaft, wurde im Zuge der BIA (Tabelle 8) wie folgt ermittelt:

„Die Nicht-Verfügbarkeit von Daten wird lediglich einen Tag toleriert, da ansonsten ein hoher Schaden zu erwarten ist.“ Standortbedingt ist mit einer erhöhten Brandgefahr zu rechnen. Um das Risiko eines Infrastrukturausfalls > 1 Tag zu reduzieren, sind zwei Gegenmaßnahmen erfasst worden:

- **A_1**: *Der Aufbau eines zweiten Rechenzentrums B an einem anderen Standort, welches bei einem Ausfall vom Rechenzentrum A, den Betrieb des Retail-Services, autonom und ohne Eingriff der internen Systemadministratoren, wiederherstellen kann.*

- **A_2**: *Der Aufbau einer zweiten Serverinfrastruktur in der Cloud bei einem namhaften Dienstleister, welche bei Ausfall des Rechenzentrums ohne Eingriff der internen Systemadministratoren, einen ebenfalls autarken Betrieb des Retail-Services gewährleisten kann.*

Es wurden folgende Entscheidungskriterien inkl. Parameter festgelegt:

- Dauer der Umsetzung
  - *Gewichtung: 25%, Goal: 9*
- Kosten der Umsetzung
  - *Gewichtung: 20%, Goal: 9*
- Mehraufwand in der Systembetreuung
  - *Gewichtung: 15%, Goal: 8*
- Geschätzte Risikominderung
  - *Gewichtung: 25%, Goal: 9*
- Änderungen im Verhalten / in der Organisation
  - *Gewichtung: 15%, Goal: 8*

Die Skalentransformation ordinaler Wertungen ist 5-stufig (siehe 5.3.2).

Die Zielertragsmatrix liegt wie folgt vor:

Kriterien	Maßnahmen	
	A1	*A2*
	Beurteilung	**Beurteilung**
Dauer der Umsetzung	3 Monate	1 Monat
Kosten der Umsetzung	Afa[8]= 120.000€	p.a. 85.000€
Mehraufwand in der Systembe-treuung	Niedrig	Mittel
Geschätzte Risikominderung	Gut	Sehr Gut
Änderung im Verhalten / in der Organisation	Niedrig	Mittel

Tabelle 17: Zielertragsmatrix Maßnahmenentscheidung

Berechnung des Nutzwertes mittels Nutzwertanalyse:

Kriterien	Gewich-tung	Maßnahmen			
		A_1		A_2	
		Beurteilung	**TNW**	**Beurteilung**	**TNW**
Dauer der Umsetzung	25%	3,33	0,8325	10	2,5
Kosten	20%	7,08	1,416	10	2
Änderungen in Prozessen / Systemen	15%	7,5	1,125	5	0,75
Geschätzte Risikominde-rung	25%	7,5	1,875	10	2,5
Änderungen im Verhalten / in der Organisation	15%	7,5	1,125	5	0,75
Nutzwertsumme			**6,3735**		**8,5**

Tabelle 18: Zielertragsmatrix NWA Maßnahmenentscheidung

Berechnung der geringsten Abweichungssumme mittels Goal-Programming:

Kriterien	Goals	Maßnahmen	
		A_1	A_2
		B	**B**
Dauer der Umsetzung	9	5,67	1
Kosten der Umsetzung	9	1,92	1
Änderungen in Prozesses / Systemen	8	0,5	3
Geschätze Risikominderung	9	1,5	1
Änderungen im Verhalten / in der Organisation	8	0,5	3
Summe der Abweichungen		**10,09**	**9**

Tabelle 19: Zielertragsmatrix Goal-Programming; Maßnahmenentscheidung

<u>Vergleich Nutzwertanalyse und Goal-Programming:</u>

Wie zu erkennen ist, ist bei beiden Entscheidungsregeln Alternative 2 zu wählen, was jedoch dem Beispiel geschuldet ist und nicht immer der Fall sein muss. Eine identische Zielertragsmatrix kann durchaus unterschiedliche Ergebnisse liefern, da die grundlegende Entscheidungslogik beider Verfahren sehr differiert.

Die Nutzwertanalyse ermöglicht durch ihre simple Funktionsweise eine rasche Gegenüberstellung mehrerer Alternativen. Durch die Möglichkeit der Kriteriengewichtung lassen sich unternehmensspezifische bzw. persönliche und strategische Aspekte in die Nutzwertberechnung miteinbinden. Die Funktionsweise der Zielprogrammierung erlaubt dies nur bedingt über das Festlegen der optimalen Ziele. Hierfür werden klare Aussagen zu den zu erstrebenden Zielen benötigt, wie es etwa beim Kriterium „angestrebter Reifegrad“ der Fall sein würde. Setzt man für eine Alternative z.B. das Ziel den Reifegrad des Controls von 2 auf 3 zu erhöhen, so wäre würde eine Maßnahme, welche dieses Kriterium erfüllt bereits als optimal gesehen werden.

An diesem Beispiel lassen sich nun, je nach Verfahren, folgende Rückschlüsse ziehen:

Bei der Zielprogrammierung wäre eine Maßnahme, welche den Reifegrad sogar auf 4 erhöht, bereits mit einer Abweichung von 1 zur erstrebten Zielsetzung zu bewerten. Eine Alternative, welche ansonsten idente Bewertungen der Kriterien aufweist und den Reifegrad lediglich von 3 erfüllt, würde also nach dem Prinzip des Goal Programmings, der augenfällig, besseren Alternative vorzuziehen sein.

Dieses Entscheidungsproblem wäre mit der Nutzwertanalyse vorteilhafter bewältigt worden, da jene Gegenmaßnahme mit dem höheren Reifegrad, gleichermaßen in einem höheren Nutzwert resultieren würde.

Vorsicht vor einer Generalisierung ist durch folgende These geboten:

Nicht immer bringt ein theoretisch, höherer Teilnutzen, auch einen realen, höheren Teilnutzen!

Am vorigen Beispiel resultierte die längere Umsetzungsdauer von A_1, in einer extremen Abweichung bzw. in einem geringeren Teilnutzen, wodurch A_2 einen massiven „Vorsprung“ gewann. Wäre sogar eine Umsetzungsdauer von vier Monaten tolerierbar, so hält sich der reale Nutzen in Grenzen. Folglich müssten beide Kriterien analog bewertet werden.

6 Ergebnisse der Arbeit

Im Anschluss werden die Ergebnisse der Arbeit dargelegt und die Forschungsfragen aus der Zielsetzung beantwortet:

Kann die Verwendung einer Nutzwertanalyse oder einer Zielprogrammierung zur transparenteren Risikosteuerung im IT-Risikomanagement beitragen?

Welcher entscheidungstheoretische Ansatz ist im operativen IT-Risikomanagement besser geeignet?

Abschließend werden die gewonnenen Erkenntnisse kritisch reflektiert.

Zusammenfassend lassen sich folgende Ergebnisse anführen:

Sowohl bei Verwendung der Nutzwertanalyse, als auch bei der Zielprogrammierung lassen sich qualitative und quantitative Zielgrößen behandeln und beide Verfahren sind zur Lösung multikriterieller Entscheidungsprobleme gedacht. Durch die systematische Strukturierung des Entscheidungsproblems, ist die Nutzwertanalyse leicht verständlich und gut nachvollziehbar. Es lassen sich nahezu alle Größen und Kriterien miteinander vergleichen, wodurch die Flexibilität des Verfahrens hervorzuheben ist. Besitzt der Entscheidungsträger genauere Vorstellungen über die für ihn optimale Handlungsalternative, so kann mit Hilfe des Goal-Programmings jene Alternative gefunden werden, welche dem Optimum am ehesten entspricht. Durch die Festlegung konkreter Ziele lässt sich jene Handlungsalternative mit den geringsten Abweichungen zum Optimum finden. Die erwies sich jedoch als etwas impraktikabel, da eine exakte Zielfestlegung im Risikomanagement schwierig durchzuführen ist. Der Risikoträger würde in der Praxis dazu neigen, alle Kriterien mit dem Ziel der bestmöglichen Erfüllung zu werten. Dies würde im Extremfall, ohne einer realistischen Einschätzung, in einer Zielmaximierung enden (z.B. Risikominderung, Kostenreduktion, geringste Umsetzungsdauer).

Hier ist das Prinzip der Zielgewichtung im Zuge einer Nutzwertanalyse um einiges zweckmäßiger. Durch die Gewichtung einzelner Kriterien können unter anderem auch strategische Aspekte des Unternehmens berücksichtigt werden und in die Auswahl entsprechender Gegenmaßnahmen miteinfließen. Demgegenüber steht die Möglichkeit einer gezielten Manipulation, durch eine bewusste, auf persönliche Präferenzen basierende, Gewichtung der Kriterien.

Aufgrund der einleitend erwähnten Komplexität der Entscheidungsfindung aus mehreren Alternativen und dem Fokus einer transparenten Maßnahmenentscheidung, kann folgender Standpunkt vertreten werden: „Trotz der in der Bewertung liegenden Manipulationsmöglichkeiten wird man mindestens davon ausgehen können, dass die Nutzwertanalyse, abgesehen vom Vorteil der Nachvollziehbarkeit und damit Überprüfbarkeit, vor allem bei Entscheidungen mit einer Vielzahl von Konsequenzen zu einem besser abgesicherten Urteil führt als eine intuitive Globalbewertung.“[63]

6.1 Beitrag der entscheidungstheoretischen Ansätze im operativen IT-Risikomanagement

Der Einsatz von renommierten Methoden aus der Entscheidungstheorie im operativen IT-Risikomanagement erwies sich nur bedingt als nützlich. Auch wenn die behandelten Verfahren das wesentliche Entscheidungsproblem versuchen zu lösen, so muss diese Lösung nicht zwangsläufig die Beste sein. Sowohl die Nutzwertanalyse, als auch die Zielprogrammierung kann zur transparenten Risikosteuerung beitragen. Es ist für den IT-Sicherheitsverantwortlichen eine praktische und zum Risikoprotokoll ergänzende Möglichkeit, Maßnahmenentscheidungen an die Führungsebene zu repräsentieren oder zu unterstreichen. Eine vollständige Antwort auf die Frage, welche der beiden entscheidungstheoretischen Ansätze besser zur Steuerung von Risiken geeignet ist, kann mit dieser Arbeit nicht gegeben werden. Beide Verfahren lassen den realen Nutzen unberücksichtigt, weshalb dieser vom IT-Sicherheitsverantwort-

[63] (Wirtschaftslexikon24, 2015).

lichen unbedingt, vor Implementierung der Gegenmaßnahmen, hinterfragt werden sollte.

Abschließend, sei aufgrund der höheren Flexibilität und der besseren Vergleichbarkeit von unterschiedlichen Kriterien, der Nutzwertanalyse eine bessere Eignung im operativen IT-Risikomanagement zuzusprechen.

6.2 Kritische Betrachtung und Konsequenzen

Nicht jede Maßnahme, die für sich selbst gesehen das Einzelrisiko eines Risikoszenarios verringern kann, muss eine gute Wahl im ganzheitlichen Systemumfeld darstellen.[64] Weder die Nutzwertanalyse, noch die Zielprogrammierung kalkulieren Skaleneffekte oder Zielkomplementaritäten mit ein. Jede Maßnahme wird für sich selbst anhand der definierten Kriterien bewertet, ohne eine Kombination aus mehreren Gegenmaßnahmen zu berücksichtigen. Die Nutzwertanalyse kann zwar helfen, Entscheidungen nachvollziehbar und transparent zu gestalten, jedoch lässt sich an der Subjektivität der Entscheidung zweifeln. Die frei wählbare Gewichtung kann nicht nur zur Einbindung strategischer Aspekte genutzt werden, sondern auch um persönliche Präferenzen stärker mit einfließen zu lassen. Überdies ist es sehr wichtig, das Entscheidungsumfeld genauestens zu spezifizieren: „Wo keine ausreichende inhaltliche Begründung der Kriterienwahl, Gewichtungen, Kriterienbewertungen, Art der verwendeten Skalen […] stattfindet bzw. möglich ist, bringt weder die formale Transparenz der NWA noch der Rückgriff auf Urteilspersonen ein sinnvolles Ergebnis (die äußere Form täuscht über inhaltliche Mängel).“[65]

[64] Vgl. (Harich, 2015).

[65] (Lengwenat, 2013).

Index

Literatur

BITKOM. 2006. *IT-Risiko- und Chancenmanagement im Unternehmen.* Berlin : s.n., 2006. S. 4.

BSI. 2015. bsi.bund.de. [Online] [Abgerufen am 9. 12. 2015]. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/Webkurs1004/3_BusinessImpactAnalysieren/BIA_node.html.

—. 2016. bsi.bund.de. [Online] [Abgerufen am 13. 1. 2016]. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/Webkurs1004/4_RisikenAnalysieren/2_Risiken%20bewerten/RisikenBewerten_node.html.

Duden. 2015. Risiko. [Online] [Abgerufen am 11. 9. 2015]. http://www.duden.de/rechtschreibung/Risiko.

Fink, Alexander und Siebe, Andreas. 2011. *Handbuch Zukunftsmanagement: Werkzeuge der strategischen Planung und Früherkennung.* Frankfurt/New York : Campus Verlag GmbH, 2011. S. 339.

Fleßa, Steffen. 2015. Konzepte der Entscheidungstheorie. s.l. : Universität Greifswald, [11. 12. 2015].

Gabler, Springer Verlag. 2015. Gabler Wirtschaftslexikon. [Online] [Abgerufen am 26. 10. 2015]. http://wirtschaftslexikon.gabler.de/Definition/risikomanagement.html.

—. 2016. Gabler Wirtschaftslexikon. [Online] [Abgerufen am 5. 1. 2016]. http://wirtschaftslexikon.gabler.de/Archiv/143831/nutzwert-v5.html.

—. 2015. Gabler Wirtschaftslexikon. [Online] [Abgerufen am 9. 10. 2015]. http://wirtschaftslexikon.gabler.de/Archiv/56961/entscheidungstheorie-v8.html.

Hämmerle, Matthias. 2016. To BIA or not to BIA: That is the Question ! [Online] [Abgerufen am 4. 1 2016]. http://www.bcm-news.de/2012/07/30/to-bia-or-not-to-bia-that-is-the-question/.

Harich, Thomas W. 2015. *IT-Sicherheit im Unternehmen.* 1. s.l. : mitp-Verlags GmbH & Co. KG, 2015.

—. 2015. *IT-Sicherheit im Unternehmen.* s.l. : mitp.Verlags GmbH & Co. KG, 2015. S. 28.

—. 2015. *IT-Sicherheit im Unternehmen.* s.l. : mitp-Verlags GmbH & Co. KG, 2015. S. 29.

ITWissen. 2015. Bedrohung. [Online] [Abgerufen am 11. 11. 2015]. http://www.itwissen.info/definition/lexikon/Bedrohung-threat.html.

—. 2015. Schwachstelle. [Online] 2015. [Abgerufen am 8. 11. 2015.] http://www.itwissen.info/definition/lexikon/Schwachstelle-vulnerability.html.

Jacob, Michael. 2012. *Informationsorientiertes Management.* Kaiserslautern : Springer Gabler, 2012. S. 101.

Krallmann, Hermann, Frank, Helmut und Gronau, Norbert. 2002. *Systemanalyse im Unternehmen.* München : Oldenbourg Wissenschaftsverlag GmbH, 2002. S. 95.

Kühnapfel, J. 2014. *Nutzwertanalysen in Marketing und Vertrieb.* s.l. : Springer, 2014. S. 41.

Meixner, Oliver und Haas, Rainer. 2010. *Wissensmanagement und Entscheidungstheorie.* 2. Wien : Facultas Verlags- und Buchhandels AG, 2010. S. 93.

MITSM. 2016. *ISO 27001 Wissen.* s.l. : Munich Institute for IT Service Management, 12. 1 2016.

Obermaier, Robert und Edgar, Saliger. 2013. *Betriebswirtschaftliche Entscheidungstheorie: Einführung in die Logik individueller und kollektiver Entscheidungen.* München : Oldenbourg Wissenschaftsverlag GmbH, 2013. S. 18.

Read, Marcel. 2016. Business Impact Analyse. [Online] [Abgerufen am 5. 1. 2016]. http://www.brainguide.de/upload/publication/70/ltuq/965ed8687d6259c2d24a21a3fceb59ba_1311535400.pdf.

Schmidt, Klaus. 2006. *Der IT Security Manager.* s.l. : Hanser Verlag, 2006. S. 21.

—. 2006. *Der IT Security Manager.* s.l. : Hanser Verlag, 2006. S. 22.

Seibold, Holger. 2006. *IT-Risikomanagement.* München : Oldenbourg Wissenschaftsverlag GmbH, 2006. S. 79.

—. 2006. *IT-Risikomanagement.* München : Oldenbourg Wissenschaftsverlag GmbH, 2006. S. 109.

—. 2006. *IT-Risikomanagement.* München : Oldenbourg Wissenschaftsverlag GmbH, 2006. S. 12.

—. 2006. *IT-Risikomanagement.* München : Oldenbourg Wissenschaftsverlag GmbH, 2006. S. 135.

Stelling, Johannes N. 2009. *Kostenmanagement und Controlling.* München : Oldenbourg Wissenschaftsverlag GmbH, 2009. S. 319.

—. 2009. *Kostenmanagement und Controlling.* München : Oldenbourg Wissenschaftsverlag GmbH, 2009. S. 313.

—. 2009. *Kostenmanagement und Controlling.* München : Oldenbourg Wissenschaftsverlag GmbH, 2009. S. 322.

Vorest AG. 2014. ISMS-ISO 27001. [Online] [Abgerufen am 29. 12. 2014]. http://www.iso27001-it-sicherheit.de/isms/risikoanalyse/.

Wirtschaftslexikon24. 2015. Wirtschaftslexikon24.com. [Online] [Abgerufen am 8. 12. 2015]. http://www.wirtschaftslexikon24.com/d/goal-programmierung/goal-programmierung.htm.

Zelewski, Stephan und Peters, Malte. 2005. *Goal Programming zur Lösung von Zuordnungsproblemen.* Essen : WISU, 2005. S. 1.

Anlagen

Anlagen, Teil 1

Business Impact Confidentiality			**3 - High**
BI-ID	**Business Impact Dimensions**	**Description**	**Impact**
C-1	Protection of personal data	*Breach of confidentiality of customer data can have a high impact.*	3- High
C-2	Legal Breaches	*Loss of data confidentiality can result in legal issues*	3- High
C-3	Breaches of rules and regulations	*Rules and regulations to keep processed data confidential are not formalized.*	2- Medium
C-4	Breach of contracts	*Breach of contracts is not applicable as partner stores do not exist in relevant country.*	0- n/a
C-5	Impairment of business processes	*The loss of confidentiality causes irritations to business processes.*	1- Low
C-6	Negative external effects	*Data leakage can lead to a loss of reputation.*	3- High
C-7	Competitive disadvantage and intangible damage	*Certain data, like sales per location are valuable for competitors.*	3- High
C-8	Personal safety	*not applicable*	0- n/a
A-9	Financial consequences	*Financial consequences due to breach of confidentiality include penalties from the government and sales shortfalls from competitive disadvantages and dissatisfied customers.*	2- Medium

Anlagen, Teil 2

Business Impact Integrity/ Authenticity			**3 - High**
BI-ID	**Business Impact Dimensions**	**Description**	**Impact**
I-1	Protection of personal data	*Personal data needs to be stored and transmitted correctly by the application as customer data is processed (including purchase history) which entails bonuses in case of exceeding certain thresholds.*	3- High
I-2	Legal Breaches	*Legal requirements to process data correctly and prove correctness exist as sales are the basis for tax calculation.*	3- High
I-3	Breaches of rules and regulations	*Internal Rules and Regulations request correct data due to Internal Audit and Reporting obligations. (Quality Checks)*	3- High
I-4	Breach of contracts	*Breach of contracts is not applicable as partner stores do not exist in relevant country..*	0- n/a
I-5	Impairment of business processes	*A medium impact on business processes is expected in case of non- integrity due to additional work and possible overtime of employees to correct data.*	2- Medium
I-6	Negative external effects	*In case of incorrect data, customers would notice as their purchase history or voucher redemption might not be accurate. Furthermore, in case wrong data calculates stock requests, certain items might not be available for purchase when needed.*	2- Medium
I-7	Competitive disadvantage and intangible damage	*In case, items are not available due to wrong stock calculations, customers might prefer to buy at the competitor.* *Wrong prices and voucher errors in the system can result in a damaged reputation which can lead to customer churn.*	3- High
I-8	Personal safety	*not applicable*	0- n/a
A-9	Financial consequences	*Wrong data can impede sales and customer loyalty and therefore impacts the business highly.*	3- High

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Baumkirchen, den 18.01.2016

Christopher Petz